MEDSTSEAD PARISH COUNCIL

DATA BREACH POLICY

1. Introduction

1.1. Medstead Parish Council is a Data Controller, as defined by GDPR legislation. The Parish Council has a legal duty to keep the personal data it holds secure and to put in place the appropriate procedural, organisational and technical measures to prevent data breaches. Despite this, data breaches may occur.

1.2. The Council needs to be able to identify when a data breach has occurred and it needs procedures in place to be able to quickly investigate it and know what needs to be reported, to whom and when. It needs to be clear what individuals'roles and responsibilities are and what other actions it needs to take.

2. Scope

2.1. The Council handles other confidential data besides personal data and the Council also needs to hold that secure. However, this policy deals just with personal data, as defined in the UK GDPR.

2.2. This policy should be read in conjunction with the Council's Data Protection Policy.

3. Definition of Personal Data

3.1 For a definition of personal data, (including special categories of personal data) and the Council's obligations under the Data Protection Act 2018 and UK GDPR, refer to the Council's overall Data Protection Policy.

4. Definition of a Personal Data Breach

4.1 UK GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

4.2 Medstead Parish Council Parish Council takes the security of personal data seriously: computers, email, website access, cloud-based accounting and HMRC submissions are all password protected and the computer is protected against viruses, data is backed up and hard copy files are kept in locked cabinets. The Data Protection Policy identifies measures intended to minimise the risk of data breaches and the IT policy details technical measures to minimise security threats and the risks of accidental loss.

5. Consequences of a personal data breach

5.1 UK GDPR notes that if a Personal Data breach is not addressed in an appropriate and timely manner, it can result in "physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of

confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

5.2 Therefore, a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

6. Roles and responsibilities

6.1 The Council's overall Data Protection Policy identifies roles and responsibilities. As a corporate body, the Council is collectively a Controller responsible for managing the processing of personal data and investigating and reporting data breaches. However, this role is delegated to the Clerk on a day to day basis.

6.2 The Council has appointed two Data Protection Lead Councillors to ensure adequate expertise within the Council and these will play a kay advisory role. Whilst other Councillors will also be able to provide guidance, having focussed expertise is intended to help the Council respond quickly when needed.

6.3 In the event of a breach it is not possible to delegate decision-making responsibilities to individual Councillors and the Council will not be able to arrange a legally-convened meeting with three clear days' notice in the timescales needed to respond. Therefore, the Council delegates the authority to the Clerk to act and make decisions in the event of a breach of data breach.

7. Procedures for dealing with a data breach

7.1 The Clerk is likely to be the first to discover a data breach, but if a Councillor or another employee (should there be one) discovers it first, they should inform the Clerk as soon as possible. The Clerk will then immediately inform the Data Protection Lead Councillors and the Chairman. These actions should take place even at evenings or weekends where necessary and if feasible.

7.2 The Clerk will obtain as much information as possible from the person reporting the breach. The Clerk and Lead Councillors will collaborate in establishing the likelihood and severity of the risk to people's rights and freedoms, referring to the guidance published by the Information Commissioner's Office (ICO). This step will determine whether the Council needs to notify the ICO and the individuals affected by the breach.

7.3 ICO guidance states that the Parish Council (as a Data Controller) should notify the ICO of a breach unless it is able to demonstrate that it is unlikely to result in a risk to the rights and freedoms of individuals.

7.4 A risk to individual's rights and freedoms may not automatically occur if the Council has implemented appropriate technical measures (i.e. encryption) that have rendered the personal data unintelligible to any person not authorised to access it or it has taken other suitable actions to mitigate risks.

7.5 The Council holds a Record of Processing Activity for all personal data held which will be used to help quickly identify the implications of a data breach.

7.6 If the decision is made that a data breach is considered likely to result in a risk to the rights and freedoms of the individuals, it is Clerk's responsibility to inform the ICO.

7.7 The data breach should be reported via the ICO website without undue delay and within 72 hours of the time that the Council became aware that the breach occurred.

7.8 If the ICO is not informed within 72 hours, the Clerk must give the ICO reasons for the delay when they report the breach.

7.9 The decision to notify or not notify the ICO and individuals involved could have implications for the Council, such as costs of notifying people, legal liabilities, and potential fines for taking incorrect action. It could also affect the reputation of the Council. Therefore, the Clerk should seek advice from the Lead Councillors, the Chairman and also the rest of the Council if appropriate and feasible.

7.10 The Clerk should aim to keep the whole Council abreast of what is going on if there is a significant breach, but also needs to stay focused on dealing with the matter than get side-tracked by excessive internal communication.

7.11 The Clerk should consider the need to call an extraordinary meeting as soon as possible, as even if this cannot be done in the timescales needed to respond to the ICO, there will likely be follow-up issues that will need addressing.

7.12 Where it has been agreed that a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s) concerned, the Clerk should inform the data subject(s) of the breach without undue delay in order to allow them to take the necessary precautions to protect themselves from the potential effects of the breach.

7.13 Where it is concluded that there is not a risk to people's rights and freedoms then the breach will not be reported to the ICO or individuals.

7.14 The Clerk will make a clear record of the reasons for either reporting or not reporting the breach.

7.15 The Clerk and Councillors will ensure that it takes any steps it immediately can that can contain the breach and minimise the potential risk of harm to the people whose data has been breached.

7.16 Any measures needing spending decisions (if exceeding the emergency delegated spending limit of the Clerk or Chairman) or any other decisions outside of the basic steps agreed in this policy will require an extraordinary meeting. E.g. payment for IT consultancy, new laptop etc.

8. Informing the Information Commissioner's Office

8.1 When notifying the ICO of a breach, the Clerk (on behalf of the Council) must:

- Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- Communicate the name and contact details of the Council's representative (the Clerk)
- Describe the likely consequences of the breach
- Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate possible adverse effects

8.2 The Clerk and Council will also consider whether it would be appropriate to notify third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

9. Review of the Data Breach

9.1 Following the immediate protective measures and reporting, the Clerk and Lead Councillors will then carry out an investigation to determine how the breach occurred, whether any Council policies were breached and by whom, and what measures can be put in place to reduce the risk of a similar breach occurring in the future.

9.2 If the breach is deemed to be due to any action or inaction by an employee or councillor, then there will be an assessment of whether it will be appropriate to invoke the Parish Council's Disciplinary Policy (for staff) or the Code of Conduct Policy (for Councillors).

10. The role of external Data Processors

10.1 The only organisations that routinely process data on behalf of Medstead Parish Council are HMRC, Vision ICT for webhosting and email provision, and Scribe as the accounting software provider and banks.

10.2 These organisations have a legal duty to inform Medstead Parish Council Parish Council if they become aware of a personal data breach that affects the Council without undue delay. It is then Medstead Parish Council's responsibility to inform the ICO and any affected data subjects.

11. Records of data breaches

11.1 All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data. Records of data breaches should include the following:

- Date of breach
- Type of breach
- Facts relevant to the breach and its effects
- Number of individuals affected
- Date reported to ICO/individuals
- Reasons for reporting the breach or not reporting the breach to the ICO or individuals if determined unnecessary
- Remedial actions to prevent breach recurring

12. How to report a data breach to the Information Commissioner's Office

11.1 To report a data breach to the ICO, Medstead Parish Council should use the ICO online system: https://ico.org.uk/for-organisations/report-a-breach/

Version Control

Version	Date adopted	Minute ref.
Data Breach Policy 2026	First adopted 22nd January 2026	26.103 (c)