MONKSILVER PARISH COUNCIL DATA PROTECTION & INFORMATION MANAGEMENT POLICY

1. **ABOUT THIS POLICY**

1.1 This policy outlines the standards Monksilver Parish Council ('the Council') intends to observe in relation to its compliance with the General Data Protection Regulations (GDPR) and subsequently revised UK Data Protection law.

1.2 The Policy is applicable to all councillors and any employees, partners, voluntary groups, third parties and agents authorised by them.

1.3 The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

1.4 This policy applies to all personal information created or held by the Council, in whatever format. This includes, but is not limited to paper, electronic, mail, photographic and video.

2. RESPONSIBILITIES

2.1 To operate efficiently, the Council must collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, contractors, suppliers, voluntary groups and partner organisations.

2.2 The Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business. The Council will, therefore, ensure that it treats personal information correctly in accordance with the law.

2.2 The Council as a whole is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to the Parish Clerk, who will undertake information audits and manage the information collected by the Council including the issuing of privacy notices, dealing with requests and complaints raised and the safe disposal of information.

2.3 Councillors who process personal data on an individual basis and are not acting on behalf of the Council are likely to be considered data controllers and therefore required to notify the Information Commissioner's Office.

2.4 All councillors and officers who hold or collect personal data are responsible for compliance with data protection legislation and must ensure that personal and/or sensitive information is kept and processed in accordance with this policy.

3. BREACH OF THIS POLICY

3.1 Breach of this policy may result in disciplinary action in accordance with the Council's Conduct procedures and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal and/or cancelled contract. It should also be noted that breach of the policy could also lead to criminal or civil action if legal material is involved or legislation is contravened. Councillors found to be in breach of this policy may also be deemed to have breached the Code of Conduct and referred to the Somerset Council's Monitoring Officer.

4. **PRIVACY BY DESIGN**

The GDPR requires data controllers to put in place measures to minimise personal data processing and that they only process data that is necessary for the purposes of processing and stored for as long is necessary.

4.1 The Council will have the appropriate measures in place to determine the basis for lawful processing and will undertake risk assessments to ensure compliance with the law. These measures include the use of Data Protection Impact Assessments (DPIAs).

5. CONTRACTS

5.1 Data protection law places requirements on both the Council, its partner organisations and its suppliers and contractors to ensure the security of personal data, and to manage individuals' privacy rights. Whenever the Council uses a supplier or contractor to process individuals' data on its behalf it must have a written contract in place.

5.2 The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

5.3 The Council is liable for its compliance with data protection law and must only appoint suppliers and contractors who can provide 'sufficient guarantees' that the requirements of the law will be met, and the rights of individuals protected.

5.4 If a contractor, partner organisation or agent of the Council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the Council, or if they will do so as part of the services they provide to the Council, the relevant lead Councillor or Clerk must ensure that personal data is managed in accordance with data protection law and this policy.

5.5 Security and data protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council and reviewed during the contract's life cycle.

5.6 The lead Councillor and the Clerk will use the appropriate processes, templates and DPIAs when managing or issuing contracts.

6. INFORMATION SHARING

6.1 The Council may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

6.2 Information must always be shared in a secure and appropriate manner and in accordance with the information type. The Council will be transparent and as open as possible about how and with whom data is shared, with what authority, and for what purpose, and with what protections and safeguards.

6.3 Any Councillor or clerk dealing with telephone enquiries must be careful about disclosing personal information held by the Council. In order to manage, this the enquirer will be asked to put their request in writing in the first instance.

7. INDIVIDUALS RIGHTS

7.1 An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject to Access Request (SAR). Information on how an individual can make a SAR can be obtained by requesting from the Parish Clerk in writing at the address at the end of this document.

7.2 Individuals also have other rights under the Data Protection Act 2018 which are set out in the Councils privacy notice. The Council must respond to individuals exercising their rights within one month.

8. DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

8.1 Personal data can only be discussed about a third party in accordance with the Data Protection Act 2018.

8.2 if a user believes it is necessary to disclose information about a third party to a person requesting data, they must seek specialist advice from Somerset Association Local Councils before doing so.

9. **BREACH OF INFORMATION SECURITY**

9.1 The Council understands the importance of recognising and managing information security incidents. This occurs when data or information is transferred to somebody who is not entitled to receive it. It includes losing data or theft of information, unauthorised use of the Council's system to process or store data by any person or attempted unauthorised access to data or information regardless of whether this was successful or not.

9.2 All users have an obligation to report actual or potential data protection compliance failures as soon as possible and take immediate steps to minimise the impact and to assist with managing risk. The Council will fully investigate both actual and potential failures and take remedial steps if necessary, and maintain a register of compliance failures. If the incident involves or impacts personal data it must be reported to the Information Commissioners Office (ICO) within 72 hours.

10**. IT AND COMMUNICATION SYSTEMS**

10.1The Council's IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards users must observe when using these systems and practices and the action the Council will take if users breach these standards.

10.2 Breach of this policy may be dealt with under the Council's Disciplinary Procedure and under the Somerset Code of Conduct for Parish Councils.

11**. EQUIPMENT SECURITY AND PASSWORDS**

11.1 The clerk is responsible for the security of the equipment allocated to them or used by them and must not allow it to be used by anyone other than in accordance with this policy. The clerk and

Councillors must ensure Passwords are set on all IT equipment, including personally owned. The passwords must remain confidential and be changed regularly.

11.2 Users must only log onto Council systems using their own username and password. Users must not use another person's username and password or allow anyone else to log on using their username or password.

12. SYSTEMS AND DATA SECURITY

12.1 Users should not delete, destroy or modify existing systems, programmes, information or data on Council equipment (except as authorised in the proper performance of their duties).

12.2 Users must not download or install software from external sources on Council equipment. Downloading unauthorised software may interfere with the Council's systems and may introduce viruses or other malware.

12.3 Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

12.4 Users must inform the Clerk immediately if they suspect a computer may have a virus.

13. **E-MAIL**

13.1 Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by email and in accordance with the Council's Communication Policy.

13.2 It should be noted that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

13.3 Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

13.4 For the purposes of Council business, users must use a designated email account in order to receive or send email correspondence.

14**. USING THE INTERNET**

14.1 Users should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral.

15 SOCIAL MEDIA

15.1 This policy is in place to minimise the risks to the Council through use of social media.

16.2 This policy deals with the use of all WhatsApp and email postings. No other form of social media is permitted. It applies to use of social media for council purposes as well as personal use that may affect Council business in any way.

16. PROHIBITED USE

16.1 Users must avoid making any social media communications that could damage the council's interest's or reputation, even indirectly.

16.2 Users must not use social media to defame or disparage the Council, Councillors, Clerk or any third party, to harass, bully or unlawfully discriminate against staff or third parties, to make false or misleading statements, or to impersonate colleagues or third parties

16.3 Any misuse of social media should be reported to the Chairman or Clerk immediately.

17. GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

17.1 Users should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf.

17.2 A data protection breach may result in disciplinary action up to and including dismissal.

17.3 The Clerk may be required to remove any social media content that the Council believes constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

18. RECORD'S MANAGEMENT

18.1 It is necessary for the Council to retain number of data sets as part of managing Council business. The Council shall apply the following framework;

19. DOCUMENT MINIMUM RETENTION PERIOD

19.1 Minutes books Indefinite

19.2 All financial and audit records, including bank statements, cheque book stubs, invoices, receipts, quotations and tenders for 20 years.

20. CONTACT DETAILS

The Clerk to the Parish Council
Adamah Cottage
8 Sunnybank
Monksilver
TA4 4HZ
clerk@monksilver.org