Southoe and Midloe Parish Council Data Protection Policy Oct 2019

1. Southoe and Midloe Parish Council is the Data Controller and the Clerk is the first point of contact for Data Protection. Parish Councils are not required to appoint a Data Protection Officer
2. The Councillor with lead responsibility for data protection is identified on the councillor responsibilities document.
3. The Parish Council was registered with the Information Commissioner's Office (ICO).
4. We have the following arrangements in place for releasing and publishing information to the public. The following information is published on our website in accordance with the transparency code:

    - Annual governance and accountability return
    - Internal audit report
    - Detailed payments of over £100 each financial year
    - Year end bank reconciliation
    - List of councillor or member responsibilities
    - Financial regulations
    - Financial risk assessment
    - Maintenance schedule
    - Risk assessment
    - Standing orders
    - Asset register
    - Code of conduct
    - Minutes, agendas and meeting papers of formal meetings

5. Paper records are held securely in locked boxes and electronic data on a password protected laptop in possession of the clerk.
6. We have the following information governance arrangements in place for sharing information, and for exchanging it securely when appropriate, with partners.

    - We share information between Councillors using e-mail, hard copies posted by hand or by mail and on the phone.
    - We do not share personal information with third parties unless required to do so by law (eg. to assist the police in an investigation) or we have the owners permission to do so.
    - Other, non-personal information is available by application to the Clerk or on our website.

7. We have procedures in place for responding to freedom of information, information sharing and data protection subject access requests. Members of the public can make their requests to the Clerk, Ramune Mimiene by email (southoe_pc@yahoo.co.uk) or telephone (01480 535265) and this is made clear on the GDPR page of the Parish Council's website. See the Subject Access Request Policy.

8. The risks to the council with regard to data are risk of theft / fire / corruption of files/ unauthorised access to discarded paperwork / electronic devices. These are addressed by using password protection of the laptop, backups of data held in fireproof file boxes, and virus protection on the Clerk's computer.

9. Councillors receive this policy that is reviewed and updated by the Council as changes occur or every three years (whichever is sooner). The Clerk has attended a GDPR training session run by CALPAC and aware of changes to the regulations through the Information Commissioners mailing list. This policy is available on our website.

Security

10. New Clerks and Councillors are made aware of the importance of checking that only relevant information is sent to the right recipient through this document. If sending an e-mail to more than one parishioner we would use Bcc to protect identities (unless the e-mail was being sent to a Parish Councillor or we had their permission to reveal their e-mail address to third parties).

11. We use encrypted, password protected devices to hold or transfer any files carrying personal information (a password protected, encrypted external hard drive).

12. The Clerk and Councillors are aware that they should carry out identity checks before giving out personal information over the telephone. They are aware that some people will try and trick them out of information over the phone. They are aware that only a limited amount of personal data should be given out over the phone and that written confirmation might be necessary

13. Confidential waste, either electronic or paper, is securely disposed of by shredding paper files and before a computer, external hard drive or any other electronic storage device is passed on, sold or destroyed the Clerk will ensure that all data is securely deleted using appropriate software eg. Windows cipher. Failure to comply with this is a major cause of enforcement notices under the DPA.

14. All computers used to access or process Council personal data eg. e-mails must have virus protection and a firewall, strong passwords (eg. not a name or whole word but first letters of a phrase). Clerk and Councillors check the settings of new software and devices and where possible, make changes which raise their level of security. For example, by disabling or removing any functions, accounts or services which they do not require. Tablets and phones used to access council e-mails and files will only use software downloaded from approved sources eg. Android PlayStore or iPhone AppStore and will be password protected. Software will be kept up to date on all devices.

15. The Clerk and Councillors will take care to check e-mails before sending to ensure they are going to correct recipients. They will also be careful not to click on links or open attachments in e-mails from unknown sources.

16. External backup devices will be unplugged from the computer when not in use to prevent unauthorised access in the event of a cyber breach.

Managing personal information

17. Clerk and Councillors know that they should only collect the personal information they need for a specific business purpose, and that the method of collection must include a privacy notice explaining who they are; what they are going to do with the information; and who it will be shared with. They know that we can't use it for anything else without their consent. They need to know how to withdraw their consent. The provider of the information must provide a positive opt in eg. returning a form, or choosing to tick a box before we can use the information.

18. The Clerk and Councillors are aware of the requirement to tell individuals about new or changed business purposes and updating their consent. eg. if we gather personal details for example for the neighbourhood plan we would ask the residents for their consent before using it for another purpose eg. advertising a village event.

19. Information is kept accurate and up to date if it is to be used. We take reasonable steps to ensure the accuracy of any personal data we obtain, we ensure that the source of any personal data is clear, we carefully consider any challenges to the accuracy of information; and we consider whether it is necessary to update the information.

20. Personal information that is no longer required is securely disposed of when it is no longer required for the purpose for which it was gathered. We review the length of time we keep personal data, we consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it; we securely delete information that is no longer needed for this purpose or these purposes; and we update, archive or securely delete information if it goes out of date. These reviews will take place as changes occur or every year in July and this is noted in the Parish Council risk assessment. This data protection policy has been updated in October 2019.

21. A data audit questionnaire will be completed by the Clerk in July each year to monitor compliance.

22. Schedules of data processing will be completed for new activities and consent forms with unsubscribe instructions will be sought where necessary.

23. A data audit questionnaire will be completed annually in July to check compliance, privacy notices and policies, the subject access request policy, retention policy and consent forms will be reviewed and updated in July each year.

24. Data breaches will be handled according to the Data Security Breach Response Policy

This data protection policy was adopted at a meeting of Southoe and Midloe Parish Council on 2nd October 2019