SHREWLEY PARISH COUNCIL

POLICY STATEMENT – DATA BREACH POLICY

The Parish Council recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Parish Council.
The Parish Council recognises its responsibility to comply with the Data Protection Act 1998 and the General Data Protection Regulations, May 2018
The acts regulate the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.
This policy applies to all records created, received or maintained by the Parish Council in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by the Parish Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

1. Care of personal data
Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.
2. What information does this policy relate to?
This policy relates to all personal and sensitive data held by the Council regardless of format.
3. Who does this policy apply to?
This policy applies to all staff, Councillors and volunteers at the Parish Council and includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Council.
4. What is the purpose of this policy?
The purpose of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data.
For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.
5. What is a data breach?
A data breach is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the Parish Council
A breach includes but is not restricted to, the following:
• Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
• Equipment theft or failure
• Unauthorised use of, access to or modification of data or information systems
• Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
• Unauthorised disclosure of sensitive / confidential data
• Website defacement
• ‘Hacking’ attack
• Unforeseen circumstances such as a fire or flood
• Human error

• Offences where information is obtained by deceiving the organisation who holds it

6. What happens if there is a data breach?

Any individual who accesses, uses or manages information on behalf of the Council is responsible for reporting data breach and information security incidents immediately to the Clerk. If the Clerk is unavailable, the incident must be reported to the Chairman. If the Chairman is unavailable the incident must be reported to the Vice Chairman.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

A report should be created which will include full and accurate details of the incident, when the breach occurred, who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved.

The Parish Council must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

7. What information should be included about the data breach?

When reporting a breach, the Parish Council must provide the following information:-

• a description of the nature of the personal data breach including, where possible:
• the categories and approximate number of individuals concerned; and
• the categories and approximate number of personal data records concerned;
• the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
• a description of the likely consequences of the personal data breach; and
• a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Parish Council must inform those concerned directly and without undue delay.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. The Parish Council will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then the risk is higher.

In such cases, the Parish Council will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Adopted by Shrewley Parish Council Monday 1st July 2019.
Review date Monday 3rd July 2023
To be reviewed July 2024