Aldbourne Parish Council

INFORMATION SECURITY POLICY
Adopted 2 June 2021
Next review 2023

Information Security Policy

Aldbourne Parish Council is committed to establishing and maintaining the security and confidentiality of information held by the parish council. This applies to all information held by staff, councillors, volunteers, and any individual/organisation under contract to the council. All those associated with the council including staff and councillors have a legal responsibility to maintain the confidentiality, integrity and security of data held. This includes information written or printed on paper, stored electronically, transmitted by post or electronic means, shown on films, or spoken in conversation. Aldbourne Parish Council recognises its responsibility to comply with the Data Protection Act 2018 & General Data Protection Regulations, which regulates the use of personal data.

Security

All personal information held by the parish council will be kept in a secure location and not available for public access. All such data stored on a computer or off-site server will be password protected. Passwords will be periodically changed. Personal data will be monitored on a regular basis and shredded or deleted once it has served its purpose, is not needed any more, or is out of date. The parish clerk is responsible for the safe storage of personal data. Information will be supplied to a councillor to help them carry out their duties, upon request. They will only receive as much information as necessary.

Confidentiality

Aldbourne Parish Council must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential. The council recognises that all staff need to be aware of information security threats and concerns, and that they will be expected to support and adhere to the councils Information Security Policy at all times.

Reporting

All staff and other users should report immediately to the clerk or Chairman of the Council: Any observed or suspected security incidents where a breach of the council's security policies has occurred; Any security weaknesses in, or threats to, systems or services.

After any breach, the parish council will establish the cause of the breach and evaluate the effectiveness of its response. It eh breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continue with 'business as usual' is not acceptable; similarly, if the parish council's response was hampered by inadequate policies or a lack of clear allocation of responsibility then there will be a review and update of these policies and lines of responsibility – light of the breach experience.

Conclusion

This policy and associated procedures will be reviewed and amended periodically or as outlined above, in the event of a security incident or other event.

The policy and procedures have been approved by the parish council.

Employees and parish councillors are obliged to comply with this policy and procedures when processing information on our behalf.

All employees and parish councillors who process personal data are required to read the policy/procedures and indicate that they understand it. If anybody requires clarification of the policy/procedures/guidelines they should speak with the clerk.