Gladestry Community Council

Data Protection and Security Policy

Personal Data stored will be emails, names, addresses and telephone numbers as supplied by the data subject during routine contact with the Council and from those making contact through the website. It will be stored as detailed below.
Information stored will not be released to any other organisation or person outside the Community Council without the express permission of the data subject.
Details of the data stored will be available free of charge on request and the Council undertakes to supply this within the statutory time limit current at the time of the request.

The Council will take all possible precautions to protect personal data and details of the security arrangements are below.

The Data Protection Act says security should be appropriate to:

the nature of the information in question; and
the harm that might result from its improper use, or from its accidental loss or destruction.

Accuracy and Relevance.

The Council will ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. Data obtained for one purpose will not be processed for any unconnected purpose unless the individual has agreed to this or would reasonable expect this.
Individuals may ask that we correct inaccurate personal date relating to them. Anyone believing that information is inaccurate should record the fact that the accuracy of the information is disputed and inform the Data Protection Officer (DPO). The Council has delegated the role of DPO to the Clerk.

Computer security.

Firewall and virus-checking is installed on the Council's computer which is used solely by the Clerk.
Security and operating updates are received automatically and input by the Clerk.
Regular back-ups of the information on the computer system are taken and kept securely in separate location.
All personal information is removed before disposing of old computers by wiping or replacing the hard drive.

Emails security.

Much of the Council's day to day operations is undertaken *via* email from outside organisations, and between the Clerk and Councillors. Activity also occurs between the Clerk and the Community website. It is rare for personal data to be the subject of email traffic; when this is the case, great care is taken to ensure that the data only reaches the intended recipient.

Data Security.

Personal data is kept secure against loss or misuse. The Clerk is the only user of the Council's password protected computer, and regular back-ups of information are taken and stored separately from the computer.

When data is stored on printed paper it is kept in a secure location. Printed data is safely disposed of when it is no longer required: the Council's Document retention Policy refers.

Personal data should never be saved directly to mobile devices such a tablets or smartphones.

Please use this Policy in conjunction with the Council's Email Contact Privacy Notice, to be found under Council Documents.

Please contact the DPO/Clerk if you require any further information. The Community website also holds the Council's Freedom of Information Policy and Document Retention and Disposal Policy, also to be found under Council Documents.

November 2022