

POULSHOT PARISH COUNCIL

DATA MANAGEMENT POLICY

The **General Data Protection Regulation** (Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such), otherwise known as the “GDPR”, is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA. The GDPR is enshrined in UK law as the **Data Protection Act 2018**

Poulshot Parish Council, its members, employees and non-voting members [of sub-committees or similar] are required to conform with these regulations. This policy sets out those measures the Council should take to conform.

“‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

Personal Information (PI) is any data attribute that may be used to identify an individual – such as a phone number, email address or name. Sensitive Personal Information (SPI) is any data attribute that may cause harm to an identified individual – such as their religion, health, sexual orientation or bank details.

Receipt, Distribution and Storage of Data

The Council needs to maintain control of all data it receives, stores and processes.

The Council will distribute data to its members, staff, agents and others on an as-needed basis via a secure and auditable mechanism. The Council uses “Box” for this purpose.

The Council will avoid distribution of Personal Information (PI) via email and will not distribute Sensitive Personal Information (SPI) via email. Box will be used for this purpose.

The Council holds a Data Protection Agreement with Box. Box is compliant with GDPR.

For purposes of the GDPR the Council retains Personal Information and Sensitive Personal Information under more than one lawful basis – Public Task and/or Consent and/or Contract and/or Legal Obligation and/or Legitimate Interests. One or more may apply in each circumstance.

Members, staff and non-voting members receiving emails and materials (e.g. hardcopy) related to their role with the Council or related to any Council business should:-

- Not distribute: Send to the Parish Clerk for distribution via Box and audit. Remove/Delete the material (once receipt is confirmed by the Parish Clerk). A personal upload area will be made available on Box to send material that is large or contains sensitive information.
- Where material received is not for wider distribution or communication is to remain between the member and the sender/provider, send a notification of the data to the Parish Clerk (containing: date received, sender, whether containing PI or SPI, location stored).
- When communicating directly with an individual other than a Council member via email please refer the individual to the Council's Privacy Notice (<http://www.poulshot.org.uk/privacy>) and ask that they reply that they "understand the privacy notice and consent to the sharing of their information with the [Parish Council] [You]".
- No Council related information should be stored outside of Box (or by exception, email), including in hardcopy format, unless agreed via the Parish Clerk (and its nature and location are recorded).
- Material should not be printed or stored unless a notification/agreement has been sent to the Parish Clerk.
- Where data has been lost, in whatever format, the Parish Clerk should be informed immediately.
- Where deletion of data is requested, the data you hold will need to be deleted within SEVEN days of the request and an acknowledgement sent to the Parish Clerk that this has been completed.
- Where personal email systems are used, settings should be confirmed for permanent deletion so that deleted material is not recoverable. For work email systems, confirm with your employer that deleted emails are permanently deleted. Advise the Parish Clerk of any non-compliance.
- Where contact information is held for Council business inform the Parish Clerk for adding to the data audit log.

- Access to Box and email services used for Council business should follow generally accepted security controls such as:-
 - Passwords of 6 characters or more
 - Two-factor authentication when used on non-personal devices
 - Logout after use
 - Screen Locks used where possible
 - Non-disclosure of passwords or passphrases.
 - Devices should be encrypted where possible
- USB devices should not be used to store Council data

Data Privacy

The Council maintains its Data Privacy Notice for the general public at the following location

<http://www.poulshot.org.uk/privacy/>

Adopted June 2018

Reviewed May 2019

For next review May 2020