

Data Breach Policy

Piddle Valley Parish Council

General Data Protection Regulations (GDPR) defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Piddle Valley Parish Council takes the security of personal data seriously. Any confidential documents forwarded to councillors must be marked ‘confidential’ and must only be received and/or stored on personal email addresses or electronic devices which are password protected. Hard copy files will be provided to councillors unable to meet these criteria, and must be kept in locked cabinets. Originals will be stored securely by the Clerk as defined by the GDPR security compliance checklist..

There is no requirement for individual councillors to store documents or information marked ‘confidential’, that is generated or used in the course of parish council business, once that business has been closed and all documents marked confidential must be destroyed. (Note that documents that are in the public domain are not confidential).

Consequences of a personal data breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore, a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

Piddle Valley Parish Council’s duty to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual or individuals, the breach must be reported to the individual(s) and ICO (Information Commissioner’s Office) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Responsible Officer (Clerk) must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, Piddle Valley Parish Council via the Responsible Officer (Clerk) must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Piddle Valley Parish Council must:

- i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- ii. Communicate the name and contact details of the Responsible Officer (Clerk)
- iii. Describe the likely consequences of the breach
- iv. Describe the measures taken or proposed to be taken to address the personal data breach including measures to mitigate its possible adverse affects.

When notifying the individual(s) affected by the breach, Piddle Valley Parish Council must provide the individual(s) with (ii)-(iv) above.

Piddle Valley Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Data processor's duty to inform Piddle Valley Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Piddle Valley Parish Council without undue delay. It is then Piddle Valley Parish Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

Records of data breaches

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Record of Data Breaches

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring

To report a data breach Piddle Valley Parish Council will use the ICO online system:

<https://ico.org.uk/for-organisations/report-a-breach/>

Version number	Purpose/change	Author	Date
----------------	----------------	--------	------

0.1	Initial draft	LSS	06/03/18
0.2	For review by PVPC	Chair PVPC	12/06/18
0.3	For use by PVPC	Chair PVPC	15/11/18

Next review date: April 2019