Onecote Parish Council, GDPR Compliance, Data Protection and Information Security Policies.

Data protection legislation requires that public bodies have a Data Protection Officer (DPO). The Data Protection Officer has overall responsibility for the day-to-day implementation of this policy. Currently, Parish Councils are exempt from the requirement to appoint a DPO but the Clerk effectively acts in this capacity.

The Clerk is the Data Controller and acts as the DPO whose responsibilities are as follows:

- ➢ Ensuring all data protection procedures and policies are reviewed on a regular basis
- ➢ Arranging data protection training and advice for Council members
- ➢ Responding to members of the public who wish to know which data is being held on them by the Council.

Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

Specific Responsibilities

There are specific responsibilities and actions that the Clerk and Council need to consider when making decisions in regards to processing personal or sensitive data. More information on these areas is provided below.

Privacy by design and Privacy Impact Assessments

Privacy by design is an approach required under data protection legislation which ensures that privacy and data protection compliance is taken into account with projects that involve personal and sensitive data from the start.

A Privacy Impact Assessment (PIA) is pivotal for ensuring compliance as they are mandatory for certain projects.

The DPO has overall responsibility for ensuring that Privacy Impact Assessments are conducted for all projects involving high risk processing of personal data. When relevant, and when it does not have a negative impact on the data subject, privacy options should be set to the most private by default.

Data audit

The DPO/Clerk will conduct regular data audits to manage and mitigate risks which will inform the Information Asset. This contains information on what data is held, where it is stored, how it is used, and retention timescales.

Awareness Training for Councillors
Councillors will receive training in Privacy and Data Protection Essentials (GDPR). All users have a personal responsibility. Further training will be provided whenever there is a substantial change in the law.

Reporting breaches
All Councillors have an obligation to report actual or potential data protection incidents. This allows the DPO/ Clerk to:

- ➢ Investigate and take remedial steps where necessary.
- ➢ Maintain a register of incidents as part of the responsibility to monitor all incidents.
- ➢ Comply with the mandatory requirement of notifying the Information Commissioners Office (ICO) of any breaches which hit the threshold as outlined by data protection legislation.

Principles

There are 6 principles at the heart of data protection legislation.

The principles state that personal data must be:

1. Processed fairly, lawfully and transparently
2. Obtained for a specific, explicit and legitimate purpose
3. Adequate, relevant and limited to what is necessary
4. Accurate and where necessary up to date

Data subjects have the right to ask that the Council corrects inaccurate personal data relating to them.

It is the responsibility of those who receive personal information to make sure so far as is possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate and up to date. If the information is found to be inaccurate, steps must be taken to put it

1. Obtained for a specific, explicit and legitimate purpose
This purpose must be outlined within the Privacy Notice. If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information. It must be made clear to the 'data subject' all the purposes that their information may be used for at the time the information is collected.

2. **Adequate, relevant and limited to what is necessary**

Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. For example a person's name and other identifying information should not be collected where anonymous information would suffice.

Only the minimum amount of personal information should be given. The person providing the information should make sure that the information is adequate for the purpose, relevant and limited.

3. **Accurate and where necessary up to date**

Any personal data processed must be accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

4. **Not kept longer than is necessary**

Data protection legislation states that data must not be held by the Council longer than is necessary.

Checks on personal data should be made at regular intervals and deleted or destroyed securely when it is no longer needed, provided there is no legal or other reason for holding it.

5. **Handled ensuring appropriate security**

Data must be kept securely to protect it against loss or misuse.

When personal information is given, it must be communicated in a secure manner. Communications must use secure email or be delivered in such a way as to ensure the information reaches the correct recipient.

Data Subject Rights

'Data subjects' have various rights under data protection legislation including a right to access personal information held about them and to have data amended where applicable. An outline of these rights is provided below.

The right of access (Subject Access Requests)

Data subjects have the right to obtain confirmation if data is being processed and then have a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, who the data will be shared with as well as details of the period for which the data will be retained.

The Council has one calendar month in which to respond to a SAR, provided all information required to carry out the request has been received from the applicant and suitable proof of identification has been supplied.

The right to rectification

Data subjects are entitled to have personal data rectified if it is inaccurate or incomplete.

The right to erasure

Data subjects have 'the right to be forgotten' and request their data be erased where there is no compelling reason for its continued processing, for example it is no longer required or data subject has withdrawn consent with no further legal grounds to process available.

The right to restrict

Data subjects have a right to request to stop processing their data when one of the following applies:

- The accuracy is contested and is being investigated
- The processing is believed to be unlawful
- Data subject requires for the purpose of a legal claim
- Data subject has objected to the processing which is currently being considered.
-

The right to be informed

Data subjects must be provided with a minimum of information regarding the collection and further processing of their personal data. Such information must be provided in a concise, Data subject has objected to the processing which is currently being considered.

The right to data portability

Data subjects are entitled to receive a copy of their personal data in a commonly used machine-readable format, and to transfer their personal data from one data controller to another or have the data transmitted directly between data controllers.

The right to object

Data subjects have the right to object to the processing of their personal data based the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

Rights in relation to automated decision making and profiling

Data subjects have the right not to be subject to decisions based solely on automated processing. Where such an automated decision has been made the data subject has a right to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

Version 2 August 2018