EAST CHALLOW PARISH COUNCIL

DATA PROTECTION POLICY

Introduction

Purpose of the policy and background to the General Data Protection Regulation ('GDPR')

East Challow Parish Council ("the Council") recognises its responsibility to comply with all relevant data protection legislation.

The purpose of this policy is to set out the Council's policy and procedures on data protection. It replaces any previous data protection policy and procedures and includes the additional requirements of GDPR which apply in the UK from May 2018. The GDPR is not intended to restrict the processing of personal data, but rather align it to the modern digital world and ensure that such processing is done in a way that protects the data subject's rights. The Government has confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement. Additionally, the Data Protection Bill 2017 is currently going through Parliament; when complete this legislation will complement and in some cases strengthen GDPR, effectively to replace the 1998 Act.

This policy will be reviewed and amended as necessary as the legislation develops.

The Council's registration number under the Data Protection Act 1998 is: ZA458287**.** This will remain in place until further advice is received from the Information Commissioner.

There is some jargon associated with this legislation; an explanation of the most common terms is shown below:

- **Consent** is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.
- **Data controller** is the person or organisation who determines the how and what of data processing; he/she determines the purposes and means of processing personal data
- **Data processor** is the person or firm that processes the data on behalf of the controller.
- **Processing data** means any operation performed on that personal data such as collection, recording, using it.
- **Data subject** is the person about whom personal data is processed.
- **Personal data** is information about a living individual which is capable of identifying that individual e.g. a name, address, email address, photo, or car registration number.
- **Privacy Notice** is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.
- **Processing** is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.
- **Sensitive personal data** is also described in the GDPR as 'special categories of data' and includes the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; biometric data; personnel and payroll data. Personnel and payroll data includes date of birth, details which may enable identity theft such as NI number, salary and bank account information and personal data such as details of family members.

For the avoidance of doubt, the GDPR applies to 'controllers' **and** 'processors'.

Identifying roles

EAST CHALLOW PARISH COUNCIL

It is a requirement of the GDPR that all members of the Council must understand the implications of GDPR and that roles and duties must be assigned. The Council has therefore adopted an Action Plan, to achieve compliance with the GDPR and any succeeding legislation.

Minimising risk

It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

Responsibilities

The Council has determined that it is the data controller and it has appointed the Clerk as the Data Protection Officer (DPO. The DPO's duties include:

- To inform and advise the Council about its obligations to comply with the GDPR and other data protection legislation;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train Councillors, conduct internal audits and manage the information collected by the Council;
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

To avoid any conflict of interest, the DPO will not determine the purposes or manner of processing personal data; these will be the responsibility of the Council.

Data protection principles

Article 5 of the GDPR requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and,
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

EAST CHALLOW PARISH COUNCIL

The GDPR requires that the Data Controller shall be responsible for, and be able to demonstrate, compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

Rights for individuals

The GDPR provides the following rights for individuals ('data subjects'):

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure (or, the right to be forgotten);
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

The right to be informed

.
The Council does have data that relates to living individuals and does process such data. The type of information the Council holds tends to be limited to name, address, and e-mail address, and in some cases, telephone number, although more detailed information is held for employees. The Council has adopted Privacy Notices for:

1. The general public, and,
2. Staff, councillors and Role Holders.

These notices provide all the information required by the GDPR and are available on application to the Council and on the website.

The right of access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. The procedure for handling 'subject access requests' is at Appendix 1.

Freedom of Information ('FOI')

Anyone has a right to request information from the Council, in its capacity as a public authority. The Council has two separate duties when responding to an FOI request:

1. To tell the applicant whether it holds any information falling within the scope of their request; and,
2. To provide that information.

For convenience, the handling of Freedom of Information ('FOI') requests is included in the procedure at Appendix 1.

Further information on any other rights of individuals is available on application to the Council or on the Information Commissioner's website at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Information Audit

EAST CHALLOW PARISH COUNCIL

The Council has carried out an Information Audit to clarify what personal data both it and Councillors holds, and where it is held. All data that is out of date, irrelevant or in contravention of the GDPR and this policy has been destroyed.

Electoral Roll

The Council is sent a copy of the electoral roll with updates through the year. The Data Protection issues associated with the electoral roll are the responsibility of Vale of White Horse District Council. The Council does not permit any unauthorised access to this data. Authorisation is restricted to the Chair and the Clerk to the Council.

Services relating to children

The Council does not provide any services directly relating to children. It is aware that should that circumstance change, the relevant Data Protection issues will need to be taken into consideration.

Sensitive personal data

The GDPR requires 'sensitive personal data' (as defined above) to be treated differently. It will be very unusual for the Council to need to handle any sensitive personal data, with the exception of contractual and payroll information for employees. Should it have to do so in other circumstances, the DPO will seek the prior agreement of the Chair of the Council and all sensitive personal data will be handled in accordance with procedures laid down by the Information Commissioner's Office.

Village surveys

Where the Council carries out village wide surveys, such as in the Neighbourhood Plan or a Parish Plan, the responses are anonymous and raw data is destroyed.

Storage of data

All council paper documents are stored in locked cabinets in the Clerk's office. All computer records are stored on a password protected computer with anti-virus software. All electronic files containing sensitive data will be password protected.

How the data is used

Data is only used for the purpose it has been supplied. Data is not passed onto a third party without the express consent of the data subject. The Council does not share or sell data, and never has done. Contact details for Councillors and the Clerk will normally be in the public domain. The Council may hold the personal information about individuals which is identified in the Council's two Privacy Notices, for the purposes identified therein. This information will be kept securely and not made available for public access.

Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of the Council's document retention policy, it will be shredded and / or securely deleted from the computer.

EAST CHALLOW PARISH COUNCIL

Appendix

1. Procedure for handling subject access and FOI requests
2. Procedure for handling data breaches

Last updated: May 2018.

Adopted by the Council on: 4 December 2019

EAST CHALLOW PARISH COUNCIL

Appendix 1

Procedure for handling subject access requests

Under the GDPR, individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this corresponds to the information that is provided in the Council's relevant privacy notice.

The following procedure will apply:

- Applications should be made to the Council's DPO. If the application is made electronically, the information must be provided in a commonly used electronic format;
- The identity of the person making the request must be provided, to the satisfaction of the DPO;
- If the Council is the controller of the data subject's personal data the information requested will be provided without delay and at the latest within one calendar month of receipt. However, the period of compliance may be extended by a further two months where requests are complex or numerous. If this is the case, the individual will be informed within one month of the receipt of the request, with an explanation why the extension is necessary;
- If the Council is not the controller of the data subject's personal data, but possibly a processor, the data subject will be informed and referred to the actual data controller;
- A copy of the information requested will be provided free of charge, but a reasonable fee may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive;
- Where a large quantity of information is requested, the individual may be asked to specify the information the request relates to. This will enable the Council to consider whether the request is manifestly unfounded or excessive.

Procedure for handling FOI requests

Anyone has a right to request information from a public authority. The Council has two separate duties when responding to these requests:

1. to tell the applicant whether you hold any information falling within the scope of their request; and
2. to provide that information.

The following procedure will apply:

- Applications should be made to the Council's DPO in writing and include the requester's real name, an address for correspondence and a description of the information requested. This may need to be clarified with the requester, including speaking with them; the timescale for compliance will not begin until the necessary clarification to answer the request has been received;
- Many requests can be dealt with by providing the requested information in the normal course of business. If it is necessary to deal with a request more formally, it is important to identify the relevant legislation:

    a. If the person is asking for their own personal data, that should be dealt with as a subject access request under the GDPR / Data Protection Act;

b. If the person is asking for 'environmental information', the request is covered by the Environmental Information Regulations 2004;
c. Any other non-routine request for information held by the Council should be dealt with under the Freedom of Information Act ('the Act').

- Response. The Council will respond to a valid request as soon it is able to do so, with a limit of 20 working days; if it is not possible to respond fully with that period, an explanation will be given. The Council is not always obliged to provide the information requested; an entire request can be refused under the following circumstances:

    1) It would cost too much or take too much staff time to deal with it;
    2) The request is vexatious;
    3) The request repeats a previous request from the same person;
    4) If releasing it would be contrary to the GDPR / Data Protection Act.

EAST CHALLOW PARISH COUNCIL

Appendix 2

Procedure for handling breaches of personal data

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes, including if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed or if someone accesses the data or passes it on without proper authorisation. It also means that a breach is more than just about losing personal data.

In the event of a suspected breach, the following procedure will apply:

- The person noticing a suspected breach will report the matter to the Council's DPO as soon as possible; the DPO will notify the Chair of the Council;
- The DPO and Chair will investigate whether a breach has occurred, and if so, of what type and magnitude, in order to determine the appropriate follow–up action. This will include:
    - Determining the reasons for the breach and rectifying any errors or omissions to prevent further breaches;
    - Assessing the likely risk to individuals as a result of a breach;
    - Informing affected individuals without undue delay about a breach when it is likely to result in a high risk to their rights and freedoms;
    - Providing advice to affected individuals to help them protect themselves from its effects;
    - Notifying the Information Commissioner (within 72 hours) if the breach warrants it. The Information Commissioner will want to know within 72 hours the potential scope and the cause of the breach, mitigation actions it is planned to take, and how the problem will be addressed.

A record of all breaches will be maintained by the DPO.