SHIPLEY PARISH COUNCIL

GENERAL DATA PROTECTION REGULATIONS 2018

Date Policy Reviewed	Date Policy Adopted
May 2018	17th May 2018
May 2019	16th May 2019

GENERAL DATA PROTECTION REGULATIONS POLICY

1. Policy statement

The General Data Protection Regulation ("GDPR") will take effect in the UK from 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by councils. Local councils and parish meetings must comply with its requirements, just like any other organisation.

The GDPR applies to all local councils and also to a parish meeting without a separate parish council because a local council and a parish meeting are public authorities. The GDPR requires councils and parish meetings to appoint a Data Protection Officer ("DPO"). This is confirmed by new data protection legislation currently being debated in parliament. For the GDPR and the new data protection legislation, the definition of public authorities is the same as that used in the Freedom of Information Act 2000 (which includes local councils and a parish meeting constituted under s. 13 of the Local Government Act 1972).

This policy supplements our Data Protection, IT, Email and Internet Policy.

2. Record Keeping

The Clerk will ensure that a data audit is carried out each year and the necessary consents are obtained.

3. Privacy Notices

The clerk will ensure that the necessary Privacy Notices are available on the Council website. There are two privacy notices in this Policy and are separate Council policies. The first is to be used for residents and members of the general public (but not for staff, councillors or anyone with a role in the local council). The second privacy notice is for staff members, councillors and anyone else with a role in the council.

4. Consent

The Clerk will ensure that consent to hold, retain and process personal data is obtained in accordance with GDPR requirements and section 2 above.

5. Breaches

One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of the council. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.

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. Employees, volunteers and members may not use information technology in any way that may call the Council into disrepute, cause it to breach confidentiality legislation or which could result in reputational damage for the Council or individuals

In the event of any breach, the Clerk will ensure that the necessary data breach form is completed as at Appendix A and that the actions to be taken are taken within the necessary time frames. The DPO should be promptly consulted once a data breach or another incident has occurred.

6. Right of Access (Subject Access Requests)

The Council has adopted a Subject Access policy.

7. DPO

The Council will appoint a Data Protection Officer if required. This role will not be undertaken by the Clerk and/or Responsible Finance Officer.

8. Data retention

The Council has adopted a Data Retention policy.

APPENDIX A – Data Breach Reporting.

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is Stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, Hacking attack, 'Blagging' offences where information is obtained by deceiving the organisation who holds it. Use this form to report such breaches.

Example: Reportable Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using the below link:

https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

Breach Containment and Recovery
Article 2(2) of the Notification Regulation states:
The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I of that Regulation. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

Date and time of Notification of Breach	
Notification of Breach to whom Name Contact Details	
Details of Breach	
Nature and content of Data Involved	
Number of individuals affected:	

Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner informed Time and method of contact https://report.ico.org.uk/security-breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed	
Assessment of ongoing risk	

Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	