SHERFIELD PARK PARISH COUNCIL

GDPR Policy

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

This policy explains to councillors, staff and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have confirmed that despite the UK leaving the European Union (EU), GDPR will still be a legal requirement. This policy explains the duties and responsibilities of the Council and it identifies the means by which the Council will meet its obligations.

Identifying the roles and minimising risk

GDPR requires that everyone within the Council must understand the implications of GDPR and that roles and duties must be assigned. Sherfield Park Parish Council is the Data Controller and it is their duty to undertake an information audit and to manage the information collected by the Council, the issuing of privacy statements, dealing with requests and complaints raised, and also the safe disposal of information.

GDPR requires continued care by everyone within the Council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the Council facing a fine from the Information Commissioner's Office (ICO) for the breach itself, and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to the Council (both financially and reputationally) and one which must be included in the Parish Council Risk Register.

Data breaches

One of the duties assigned to Sherfield Park Parish Council is the investigation of any breaches. 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, they will be notified directly.

It is unacceptable for non-authorised users to access Council IT equipment/systems using employees' log-in passwords or to use equipment while logged onto council systems. It is unacceptable for employees, volunteers and councillors to use IT equipment/systems 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.

Privacy Statement

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy statement. This is a notice to inform

individuals about what a Council does with their personal information. A privacy statement will contain the name and contact details of the data controller and the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the Council. The Council will adopt a privacy statement to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy statements must be verifiable.

Information Audit

The Data Controller must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the Council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the Council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

Individuals' Rights

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, Sherfield Park Parish Council will respond to this request within a month. The Clerk has the delegated authority from the Council to delete information. If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The Parish Council will be informed of such requests.

Children

There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the Council requires consent from young people under 13, the Council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

Summary

The main actions arising from this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection will be included on the Council's Risk Management Policy.
- The Parish Council will manage the process.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO. All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

Privacy Statement

This page informs you of our policies regarding the collection, use and disclosure of Personal Information we receive from users of the Site. We use your Personal Information only for providing and improving the Site. By using the Site, you consent and agree to the collection and use of information in accordance with this policy.

The data controller is Sherfield Park Parish Council.
Please contact the clerk via email for information – clerk@sherfieldparkparishcouncil.gov.uk

Information Collection and Use

While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personal, identifiable information may include, but is not limited to your name ("Personal Information").

Log Data

Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data"). This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics.

In addition, we may use third party services such as Google Analytics that collect, monitor and analyse this data. This data is completely anonymised and does not include personal information such as name or email address.

How long will we keep your data?

We hold the data securely in line with our document retention and management procedure. We keep all data for as long as: a) the project its collected for is in operation; b) on an ongoing basis but normally deleted after 7 years if our association with you is not active.

Communications

We may use your Personal Information to contact you with newsletters, should you opt into receive them.

Cookies

Cookies are files with a small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a web site and stored on your computer's hard drive. Like many sites, we use "cookies" to collect information. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site. Please see our Cookie Statement for more information.

Security

The security of your Personal Information is important to us but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

Adopted 13th November 2019, to be reviewed November 2020.