St Sampson Parish Council

General Data Protection Regulation 2018 (GDPR) - Compliance Policy and Practice.

This document sets out the action plan and policy for the Parish Council to meet its obligations under GDPR.

Action 1. Raising awareness.

The first stage of compliance with GDPR commenced at the public meeting of the Parish Council on 24 April 2018 when councillors were introduced to the 12 point ICO Action Plan, given a hard copy and updated on e mail advice from Cornwall Association of Local Councils Executive officer.

Further e mail guidance from the CALC on the subject was forwarded to Councillors on 18/6/2018 and 19/6/2018.

GDPR is on the Agenda for debate at our meeting on 26/6/2018.

Outline summary of obligations.

What is personal data?

This document sets out how we meet GDPR obligations. The regulations cover anything which we hold where an individual may be directly or indirectly recognised in particular and by reference to an identifier and relates to them personally including:-

Personnel files,

Contact details of individuals and organisations in the community

Contractors and other suppliers

Survey results where an individual may be identified.

How we use data.

We will only use data when we have the consent of the individual to use it and are restricted to only using it for that single function.

We process data lawfully, fairly and in a transparent manner in relation to individuals.

Data is only collected for specified, explicit, necessary and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Out of date or inaccurate data will be updated, corrected or deleted as appropriate.

Data will only be kept for as long as is necessary for the original purpose unless it is necessary to archive it in the public interest or on grounds of historical research or statistical purposes in which case the rights of individuals will be safeguarded in accordance with GDPR.

Data will be protected against unauthorised or unlawful access or loss.

How does the Freedom of Information Act affect data protection?

The Data Protection Act 1998 gives rules for handling information about people. It includes the right for people to access their personal data. The Freedom of Information Act and the Data Protection Act come under the heading of information rights and are regulated by the ICO.

When a person makes a request for their own information, this is a subject access request under the Data Protection Act. However, members of the public often wrongly think it is the Freedom of Information Act that gives them the right to their personal information, so you may need to clarify things when responding to such a request.

The Data Protection Act and the policy set out in this document exist to protect people's right to privacy, whereas the **Freedom of Information Act and our Publication Scheme** is about the Parish Council working **without unnecessary secrecy**. These two aims are not necessarily incompatible but there can be a tension between them, and we will apply careful judgement as appropriate.

When someone makes a request for information that includes someone else's personal data, we will carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the Data Protection Act in deciding whether we can release the information without breaching the data protection principles.

Action2. Determining personal data held.

An audit of data and information held commenced on 26 April 2018 and is on-going. We only keep data which is needed. We will not keep data which someone else – such a Cornwall Council - holds. The chair/vice chair and clerk will carry out a specific review of procedure for handling any material which is of a confidential or particularly sensitive nature with a presumption that such material should be destroyed as soon as practicable.

Action 3. Communicating Privacy Information.

Updates on our GDPR policy will be included in the Parish Council section of the village newsletter. We will review our current privacy notices and incorporate best practice advice from the ICO in our publications.

Action 4. Compliance with the rights of individuals.

Parish Council information is published in accordance with our Publication Scheme which is to be read in conjunction with this policy on data protection. We will clear out and destroy old council papers, information and documents which are no longer needed according to the rules below. We will only hold information which is needed and will not use information gathered for one purpose for any other purpose without specific approval. We respect the rights of individuals to be forgotten.

We respect the following rights for individuals:

the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and

the right not to be subject to automated decision-making including profiling.

We will NOT retain:-

- Planning papers, applications and related correspondence once the reason for their possession has lapsed – subject to the general retention date referred to below.
- Paid invoices beyond 7 years old.
- Consultation and survey responses for any COMPLETED plan or survey.
- Letters and correspondence from parishioners, other agencies or bodies about anything which has been concluded. The retention date for correspondence is 15 months.
- Applications, tenders and quotes for anything which is outside of the current contracts or audit.

On line and hard copy information and databases.

The Clerk is the Data Protection Officer for the council and holds our official information and databases on a part shared laptop computer with a back up drive.

Councillors may retain routine council paperwork in hard copy form or on their home or personal computers, tablets, phones etc for the purpose of transacting council business only and should weed all such material once the need for holding it has passed and in any case it should be weeded after 15 months. Weeding should include inbox, sent, draft and storage folders.

Councillors should copy all council business e mails in to the Clerk who will retain the official central record.

Action 5. Procedures for subject access requests.

The clerk will report subject access requests to the Chair or Vice chair who will sanction action to disclose data in accordance with GDPR. Action will be completed within one calendar month. A fee will not be charged unless it is manifestly unfounded or excessive, in which case we may ask for a reasonable fee for administrative costs associated with the request. Requests will be reported to the next meeting of the council but identity of the subject will not be published.

We may also refuse requests that are manifestly unfounded or excessive, in which case we will tell the subject within one month and allow right of appeal to a reviewing panel of the Chair and Vice Chair plus one other councillor plus remedies available via the ICO.

The GDPR does not cover information which is not, or is not intended to be, part of a 'filing system'. However, under the Data Protection Act 2018 (DPA 2018) unstructured manual information processed only by public authorities constitutes personal data. This includes paper records that are not held as part of a filing system. While such information is personal data under the DPA 2018, it is exempted from most of the principles and obligations in the GDPR and is aimed at ensuring that it is appropriately protected for requests under the Freedom of Information Act 2000. Our **Publication Scheme** sets out our policy for publication and access to parish council papers, minutes of meetings, reports and so on.

Action 6. Identification of lawful basis for our processing activity.

We will only gather, hold or process data for the legitimate purpose of transacting Parish Council business with openness and transparency evidenced throughout our work. We will balance the requirement for openness against the requirement for respecting privacy.

Action 7. Review of how we seek, record and manage consent concerning our records.

We will review how we seek, record and manage subject consent in accordance with GDPR.

Consent must be freely given, verifiable, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, preticked boxes or inactivity. It must also be separate from other terms and conditions, and we will have simple ways for people to withdraw consent.

Action 8. Age related data processing activity.

Our policy regarding age is that we will not seek to gather age specific data and will not use or publish age related data which may identify individuals. Where it becomes apparent that parental or guardian consent would be required in order to process any data relating to children or persons under 18 years of age we will cease to process the data and delete it.

Action 9. Procedures for detecting, reporting and investigating personal data breaches.

All councillors should keep up to date with GDPR obligations and report any concerns immediately to the Chair/Vice chair so that immediate action may be taken to resolve the issue.

We will notify the ICO of a breach 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, we will also notify those concerned directly in most cases.

Action 10. Privacy Impact Assessment and Data Protection by Design.

The GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'

This council is therefore committed to minimising the amount of personal data that we hold or process so as to minimise any potential adverse impact on privacy of people who deal with us.

Action 11. Data Protection Roles.

The Council is the Data Controller and decides on policy. The clerk acts as the Data Protection Officer for the council but does not set policy.

The clerk will complete an application to register the Council as a Data Controller.
https://ico.org.uk/registration/new

A NDP Steering Group and similar bodies may at times act as Data Processors and will work in accordance with this policy.

Council action on this plan will be led by the Chair and one councillor appointed to the role who together will oversee the work of the Clerk in managing our data and information. (Councillors Anderson and Jenkinson were appointed to lead on this in May 2018.) These two councillors have full delegated authority to act without recourse to the full council in order to be able to respond swiftly to any identified risk or breach of GDPR. They will undertake on-going monitoring of data protection issues and report to council of any issues. In addition they will carry out an annual audit and report findings to the full council at the same time as the annual risk management audit report.