



DATA PROTECTION POLICY

1. Background

- 1.1 In order to conduct its business, services and duties, Normandy Parish Council ('the Council'), processes a wide range of data, relating to its own operations and some which it handles on behalf of partners.
- 1.2 The Council, acting as custodians of personal data, recognises its legal and moral duty to ensure that all such data is handled properly and confidentially at all times. The purpose of this policy is to set out how the Council will meet its obligations.

2. Scope and Principles of Data Protection

- 2.1 The Data Protection Act 2018 and the UK GDPR (the retained version of the EU General Data Protection Regulation) regulate the processing of personal data. Personal data are any information which are related to an identified or identifiable natural person. Therefore, it can be as little as a name and address. Processing includes the obtaining, holding, using or disclosing of such information.
- 2.2 This policy applies to all personal data processing carried out by the Council, regardless of the format or location where that personal data is stored (e.g. in computerised records as well as manual filing systems, on an employee or councillor's own device).
- 2.3 When personal data is processed, it should be guided by the following principles listed below, as set out in the GDPR, which require personal data to be:
 - (a) processed fairly, lawfully and in a transparent manner;
 - (b) collected for specific, explicit, legitimate purposes and not processed further for purposes incompatible with those purposes;
 - (c) adequate, relevant and limited to what is necessary;
 - (d) accurate and, where necessary, kept up to date;
 - (e) kept for no longer than is necessary; and
 - (f) handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.
- 2.4 Consent for one type of data processing does not give councils permission to do anything else with the personal data. Where the consent is the basis for processing, e.g. to be added to an email mailing list, these consents will need to be verifiable.
- 2.5 There are additional protections for sensitive personal data e.g. data about race, religion or health, and the personal data of a child. A parent or guardian's consent must be obtained in order to process the personal data of children under 13.

3. Accountability and Responsibilities

- 3.1 Normandy Parish Council is the data controller, which determines how personal data is processed. The Council must notify the Information Commissioners Office (ICO) that it processes personal data, review the notification annually and pay the required fee.
- 3.2 The Council as a corporate body has ultimate responsibility for ensuring compliance with the data protection legislation. The Council must therefore allocate adequate resources and controls, including

training where necessary.

- 3.3 The Council must establish the required documentation to comply with, and demonstrate compliance with, data protection law, including privacy notices, data retention schedule, records of processing and records of personal data breaches.
- 3.4 The Council has delegated the day to day responsibility for implementation of data protection policies and procedures to the Clerk to the Council. The ICO has confirmed that town and parish councils do not need to appoint a Data Protection Officer although they may choose to do so.
- 3.5 The council must implement appropriate technical and organisation measures to protect personal data. Where data is processed by a third party, such as a payroll provider, the Council must choose a data processor that provides sufficient guarantees about its security measures to meet the requirements of GDPR and ensure the protection of the rights of data subjects.
- 3.6 Where there is uncertainty around a data protection matter, advice shall be sought from appropriate advisors e.g. Surrey Association of Local Councils (SALC) and / or the ICO.

4. Application to Parish Councils

- 4.1 Data protection laws affect councillors in three different capacities:
 - as members of the council, and therefore subject to the same responsibilities as employees;
 - when acting on behalf of a member of the public (casework); and
 - personally, when the rights of data subjects apply.
- 4.2 Councillors will only seek access to personal data when this knowledge is essential for them to carry out official duties, or where the data subject has authorised the access (casework). The information should only be used for its intended purpose and deleted afterwards.
- 4.3 Where the councillor can take a copy of the personal information away from the premises, or where they have remote access to the information, the council may specify the steps to keep the information secure, for example, setting out rules about how personal information on a laptop or on paper should be stored securely and who can have access to it.
- 4.4 The Council has a duty to observe data protection principles at all times and must balance this duty against the need to conduct its business in a transparent and open manner. The minutes of a meeting cannot routinely record the names or other personal data of an individual unless this is for the performance of contractual obligations, statutory powers or functions of the council or if the individual consents. In many cases, it will be fair to give the names of individuals who attended the meeting in a professional capacity. Minutes should not ordinarily include personal data relating to members of the public who attended and spoke at the meeting.
- 4.5 A Council must also apply the statutory data protection principles to its everyday internal administration. For example, the agenda and minutes of a meeting about a staffing matter should not disclose personal data without justification.

5. Keeping Records of Processing Activities

- 5.1 A useful way to keep a record of data processing activities is in the form of an Information Audit, which details the personal data held, where it came from, whether it is stored electronically or as a hard copy, the purpose for holding that information and with whom the council will share that information.
- 5.2 It is a statutory requirement that any activity where the processing of personal data presents a high risk to rights and freedoms of individuals should be assessed by conducting Data Protection Impact Assessments (DPIAs) before the activity commences. This largely involves special category personal data and CCTV.
- 5.3 Data processing activities could change from year to year, and so these records must be reviewed regularly and before the council embarks on a new activity.

6. Communicating Privacy Information

- 6.1 Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of data protection legislation. The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a council does with their personal information.
- 6.2 The Council has a generic privacy notice, which is displayed on the council website. The privacy notice should be written in clear language and contain information about what categories of data are processed, how and why data is collected and used, the lawful basis for processing the data, which organisations it is shared with, and the data subject rights over their personal data. It should advise the individual that they can, at any time, withdraw their agreement for the use of their personal data and include the contact details of the data protection lead in case of any queries.

7. Individuals' Rights

- 7.1 GDPR gives individuals enhanced rights over their personal data:
- the right to be informed
 - the right of access
 - the right to rectification
 - the right to restrict processing
 - right to data portability
 - the right to object
 - the right not to be subject to automated decision-making including profiling.
- 7.2 Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR'. Individuals can make SARs verbally or in writing. The Council's procedure for responding to subject access requests is given at Appendix A.
- 7.3 The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometimes known as the 'right to be forgotten') and a right to data portability which entitles

them to obtain a copy of their personal data or transfer it to another provider in a safe and secure way. These requests must be dealt with free of charge under most circumstances.

8. Destruction of Records

- 8.1 The Council shall apply a document retention policy and will permanently destroy both paper and electronic records securely in accordance with these timeframes.
- 8.2 The Council will ensure that any third party who is employed to securely destroy data has the necessary accreditations and safeguards.
- 8.3 If paper and electronic records are destroyed or deleted with the intention to put them beyond use, although it may be technically possible to retrieve them, in line with the Information Commissioner's Code of Practice on deleting data, this information will not be made available on receipt of a subject access request.

9. Data Breaches

9.1 A personal data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. If anyone (including a third party provider) knows or suspects a data breach has occurred, details of the alleged breach should be submitted immediately in writing to the Clerk.

9.2 Data breaches will be reported using the ICO's online system:

<https://ico.org.uk/fororganisations/report-a-breach/>.

Where there is doubt as to whether the breach is reportable, clarification shall be obtained from the ICO helpline on 0303 123 1113. The report shall be made as soon as possible and within 72 hours (daily hours not working hours) of becoming aware that an incident is reportable.

9.3 Where the breach is likely to result in a high risk to the rights and freedoms of individuals then those concerned directly will also need to be informed.

9.4 Evidence relating to personal data breaches must be retained, to enable the council to maintain a record of such breaches, as required by the GDPR.

10. Document Control

10.1 This policy is based on current information and advice. It will be reviewed at least annually and on change in legislation.

10.2 The council reserves the right to change this policy at any time without notice, so please check our website to obtain the latest copy.

Appendix A: Subject Access Requests

1. Data subjects have the right to request access to their personal data processed by Normandy Parish Council. Such requests are called Subject Access Requests (SARs).
2. SARs should be submitted in writing by e-mail or post to:

The Parish Clerk, Normandy Parish Council,
PO Box 1626, Guildford, Surrey, GU1 9GT.

Email: clerk@normandyparishcouncil.gov.uk
3. The request will be complied with within one month of receipt of the request.
4. When a data subject makes an SAR we shall take the following steps:
 - (a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
 - (b) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;
 - (c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and
 - (d) confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.
5. Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.
6. If the SAR is manifestly unfounded or excessive e.g. because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.
7. If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel: 0303 123 1113 (local rate).
8. If the applicant is dissatisfied with the way in which his/her request has been handled then he/she has the right to make a complaint in accordance with the Council's complaints procedure. If the complaint is unresolved, they have recourse to the ICO.