

1

## **Nayland with Wissington Parish Council**

# **DATA PROTECTION & INFORMATION MANAGEMENT POLICY**

## DATA PROTECTION

### 1 ABOUT THIS POLICY

**1.1** This policy outlines the standards **Nayland with Wissington Parish Council** ('the Council') intends to observe in relation to its compliance with the General Data Protection Regulation (GDPR) and subsequently revised UK Data Protection law.

**1.2** The policy is applicable to all councillors and any employees, partners, voluntary groups, third parties and agents authorised by them.

**1.3** The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

**1.4** This policy applies to all personal information created or held by the Council, in whatever format. This includes, but is not limited to paper, electronic, mail, microfiche and film.

### 2 RESPONSIBILITIES

**2.1** To operate efficiently, the Council must collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, customers, contractors, suppliers and partner organisations.

**2.2** The Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business. The Council will, therefore, ensure that it treats personal information correctly in accordance with the law.

**2.3** The Council as a whole is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to **the Clerk**, who will undertake information audits and manage the information collected by the Council including the issuing of privacy notices, dealing with requests and complaints raised and the safe disposal of information.

**2.4** Councillors who process personal data on an individual basis and are not acting on behalf of the council are likely to be considered data controllers and therefore required to notify the Information Commissioner's Office.

**2.5** All councillors and officers who hold or collect personal data are responsible for compliance with data protection legislation and must ensure that personal and/or sensitive information is kept and processed in accordance with this policy.

### **3 BREACH OF THIS POLICY**

**3.1** Breach of this policy may be deemed to have breached the Code of Conduct and appropriate action would result. It should also be noted that breach of the policy could also lead to criminal or civil action if illegal material is involved or legislation is contravened.

### **4 PRIVACY BY DESIGN**

**4.1** The GDPR requires data controllers to put measures in place to minimise personal data processing and that they only process data that is necessary for the purposes of processing and stored for as long as is necessary.

**4.2** The Council will have the appropriate measures in place to determine the basis for lawful processing and will undertake risk assessments to ensure compliance with the law. These measures include the use of Data Protection Impact Assessments (DPIAs).

### **5 CONTRACTS**

**5.1** Data protection law places requirements on both the Council and its suppliers to ensure the security of personal data, and to manage individuals' privacy rights. This means that whenever the Council uses a supplier to process individuals' data on its behalf it must have a written contract in place.

**5.2** The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

**5.3** The Council is liable for its compliance with data protection law and must only appoint suppliers who can provide 'sufficient guarantees' that the requirements of the law will be met, and the rights of individuals protected.

**5.4** If a contractor, partner organisation or agent of the Council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, or if they will do so as part of the services they provide to the Council, the relevant lead Councillor or Council officer must ensure that personal data is managed in accordance with data protection law and this Policy.

**5.5** Security and data protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council and reviewed during the contract's lifecycle.

**5.6** Council officers will use the appropriate processes, templates and DPIAs when managing or issuing contracts.

## **6 INFORMATION SHARING**

**6.1** The Council may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

**6.2** Information must always be shared in a secure and appropriate manner and in accordance with the information type. The Council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

**6.3** Any Councillor or officer dealing with telephone enquiries must be careful about disclosing personal information held by the Council.

## **7 INDIVIDUALS' RIGHTS**

**7.1** An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR). Information on how an individual can make a SAR can be found in this Council's Subject Access Request Policy.

**7.2** Individuals also have other rights under the Data Protection Act 2018 which are set out in the Council's privacy notices. The Council must respond to individuals exercising their rights within one month.

## **8 DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES**

**8.1** Personal data can only be disclosed about a third party in accordance with the Data Protection Act 2018.

**8.2** If a user believes it is necessary to disclose information about a third party to a person requesting data, they must seek specialist advice before doing so.

## **9 BREACH OF INFORMATION SECURITY**

**9.1** The Council understands the importance of recognising and managing information security incidents. This occurs when data or information is transferred to somebody who is not entitled to receive it. It includes losing data or theft of information, unauthorised use of the Council's system to process or store data by any person or attempted unauthorised access to data or information regardless of whether this was successful or not.

**9.2** All users have an obligation to report actual or potential data protection compliance failures as soon as possible and take immediate steps to minimise the impact and to assist with managing risk. The Council will fully investigate both actual and potential failures and take remedial steps if necessary maintain a register of compliance failures. If the incident involves or impacts personal data it must be reported to the ICO within 72 hours.

## **10 E-MAIL**

**10.1** Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

**10.2** It should be noted that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

**10.3** Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

**10.4** For the purposes of council business, users should use either a designated email account or set up an orderly system of folders to keep Council emails separate from other emails.

**10.5** Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

## **11 BRING YOUR OWN DEVICE (BYOD)**

The Council must take appropriate technical and organisational measures against accidental loss or destruction of or damage to personal data. Councillors/Clerk using their own devices raises a number of data protection concerns due to the fact that these are owned by the user rather than the data controller. The risks the controller needs to assess are:

- The type of data held.
- Where the data may be stored.
- How the data is transferred.
- Potential data leakage.
- Blurring of personal and business use.

- The device's security capacities.
- What to do if the person who owns the device leaves the Council and
- How to deal with the loss, theft, failure and support of a device.

Councillors and officers using their own devices shall have the following responsibilities:

- Users will not lend their device to anybody.
- Users will inform the Council should they lose, sell, recycle or change their device.
- Users will ensure all Council Personal Data is transferred/erased ahead of disposal of their device
- Users will enable a security password to access their device and an automatic lock requiring re-entry of the password.
- Users will ensure security software is set up on their device and kept up to date.
- Users must be careful when introducing new software to their devices to avoid introducing viruses or other malware.
- Users must inform **the Clerk** immediately if they suspect a device may have a virus.

## 12 RECORDS MANAGEMENT

**12.1** It is necessary for the Council to retain a number of data sets as part of managing council business. The Council shall apply the following framework :

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
<input type="checkbox"/> Minute books	Indefinite	Archive
<input type="checkbox"/> Scales of fees and charges	6 years	Management
<input type="checkbox"/> Receipt and payment account(s)	Indefinite	Archive
<input type="checkbox"/> Receipt books of all kinds	6 years	VAT

<input type="checkbox"/> Bank statements, including deposit/savings accounts	Last completed audit year	Audit
<input type="checkbox"/> Bank paying-in books	Last completed audit year	Audit
<input type="checkbox"/> Cheque book stubs	Last completed audit year	Audit
<input type="checkbox"/> Quotations and tenders	6 years	Limitation Act 1980 (as amended)
<input type="checkbox"/> Paid invoices	6 years	VAT
<input type="checkbox"/> Paid cheques	6 years	Limitation Act 1980 (as amended)
<input type="checkbox"/> VAT records	6 years generally but 20 years for VAT on rents	VAT
<input type="checkbox"/> Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)
<input type="checkbox"/> Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)
<input type="checkbox"/> Wages books	12 years	Superannuation
<input type="checkbox"/> Insurance policies	While valid	Management
<input type="checkbox"/> Certificates for Insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (Sl. 2753), Management.
<input type="checkbox"/> Investments	Indefinite	Audit, Management
<input type="checkbox"/> Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
<input type="checkbox"/> Members allowances register	6 years	Tax, Limitation Act 1980 (as amended)

<b>For Halls, Centre, Recreation Grounds</b>		
<ul style="list-style-type: none"> <li>▪ application to hire</li> <li>▪ lettings diaries</li> <li>▪ copies of bills to hires</li> <li>▪ record of tickets issued</li> </ul>	6 years	VAT
<b>For Allotments</b>		
<input type="checkbox"/> Tenancy Agreement, register and plans	Indefinite	Audit, Management
<b>For Burial Grounds</b>		
<ul style="list-style-type: none"> <li>▪ register of fees collected</li> <li>▪ register of burials</li> <li>▪ register of purchased graves</li> <li>▪ register/plan of grave spaces</li> <li>▪ register of memorials</li> <li>▪ applications for interment</li> <li>▪ applications for right to erect memorials</li> <li>▪ disposal certificates</li> <li>▪ copy certificates of grant of exclusive right of burial</li> </ul>	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (Sl. 204)