

# **NETHERWITTON PARISH COUNCIL**

## **DRAFT DATA PROTECTION & RETENTION POLICY**

**Approved:**

## **DATA PROTECTION PRINCIPLES**

- 1.1 In complying with the Data Protection Act 2018, Netherwitton Parish Council shall ensure that all data is:
  - Processed fairly, lawfully and in a transparent manner
  - Collected for specified, explicit and legitimate purposes and not processed in a manner compatible with those purposes
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
  - Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for personal data is processed
  - Processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 1.2 Where the lawful basis for processing data is consent, the council shall ensure that consent is freely given, unconditional and explicit.
- 1.3 The Parish Clerk/RFO shall take all reasonable steps to ensure the security of council data; this should include ensuring that access to data is limited and that data is disposed of securely.
- 1.4 The council does not use automated decision making or profiling of individual personal data.
- 1.5 The Parish Clerk/RFO is the nominated Data Protection Officer.
- 1.6 The council shall ensure that any third party which processes data on its behalf has sufficient data protection, security measures and breach reporting processes in place, and this shall form part of the terms and conditions of any contract entered into.
- 1.7 Data related to a child will not be processed without the express parental/guardian consent of the child concerned.
- 1.8 Members and employees must abide by any procedures developed in accordance with this policy and failure to do so may result in disciplinary proceedings or suspension of access to council resources.
- 1.9 The Parish Clerk/RFO shall ensure that a Data Audit is undertaken on a regular basis.

## **TRAINING & GUIDANCE**

- 2.1 All members and employees of the council shall receive an induction on Data Protection and training as required.
- 2.2 The Parish Clerk/RFO shall maintain a guidance note on Data Protection for both members and employees to provide easy to access guidance on Data Protection practices.

## **PRIVACY NOTICES**

- 3.1 The Parish Clerk/RFO shall prepare privacy notices as required which will be published on the Parish Council website. They should be reviewed annually. Privacy Notices may vary depending on the data being collected/held.
- 3.2 The Parish Council will use a balanced approach to provide privacy information to individuals; providing information at the point of collection and reference to the full privacy notice where it is not practical to provide the notice in full at the point of collection.
- 3.3 At collection, sufficient information will be given to detail why the data is being collected, how it will be used, how long it will be kept for and whether it will be shared with any third party.
- 3.4 Privacy notices will be prepared with reference to guidance from the Information Commissioner's Office and shall be provided in simple language, in a clear font.

## **BREACH REPORTING**

- 4.1 A data breach is defined as a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data'.
- 4.2 The Parish Clerk shall maintain procedures to safeguard against potential data breaches.
- 4.3 All data breaches shall be reported to the Parish Clerk/RFO who shall maintain a record of data breaches and determine, in accordance with the Information Commissioner's Office guidance, whether the breach must be reported.

## **DATA PROTECTION IMPACT ASSESSMENTS**

- 5.1 A Data Protection Impact Assessment is a process to identify and minimize the data protection risks of a project. It is mandatory for certain types of data processing or processing which is likely to result in a high risk to individuals' interests.
- 5.2 The Parish Clerk shall prepare procedures for determining if a Data Protection Impact Assessment is required and the undertaking of the same.

## **DATA RETENTION**

- 6.1 The Parish Council will only keep data for as long as it is necessary to do so.
- 6.2 The council's standard data retention requirements are detailed in appendix A.
- 6.3 Data (electronic or physical) should only be disposed of if reviewed in accordance with the following:
  - Is retention required to fulfil a statutory requirement or regulatory requirement?
  - Is retention required to meet the operational needs of a service?
  - Is retention required to evidence events in the case of dispute?
  - Is retention required because the document/record is of historic interest or intrinsic value?
- 6.4 All records containing personal information must be destroyed at the end of the retention period.
- 6.5 Where documents are of historical interest, it may be appropriate that they are transmitted to Teesside Archives.
- 6.6 Retention periods may be increased by government regulation, judicial or administrative constraint order, contract, pending litigation or audit requirements, and such modifications shall supersede the requirements in appendix A.

## **DATA SUBJECT RIGHTS**

- 7.1 A data subject has the right to:
  - Access their information
  - Correct information held which they believe is incorrect
  - Request information is deleted

- Object to the processing of data
- Request data is transferred to another data controller
- Withdraw consent for processing of data
- Lodge a complaint with the Information Commissioner's Office

7.2 A data subject wishing to exercise their rights may do so by contacting the Parish Clerk.

## **REVIEW & MONITORING**

8.1 This policy shall be reviewed periodically and in light of experience, comments from data subjects and guidance from the Information Commissioner's Office.

## **APPENDIX A**

### GENERAL

<b>DOCUMENT</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>REASON</b>
Signed Minutes	Indefinite	Archive, public inspection
Agendas	5 years	Management
Title Documents/Deeds	Indefinite	Audit, management
Contracts/Leases	Indefinite	Management
E-mail (excluding spam)	2 years	Management
Register of Members' Interests	1 year after end of service	Management
Strategic Plans, Annual Reports etc	Permanent archive once superseded	Common practice
Policies & Operational Procedures	7 years after superseded	Management
Legal/Litigation Files	Active plus 7 years	Management
Commercial Debt Recovery Matters	Active plus 2 years	Management
Complaints Records	6 years	Common practice

### FINANCIAL

<b>DOCUMENT</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>REASON</b>
Audited Accounts	Indefinite	
Accounting Records (invoices, VAT records etc)	6 years	VAT
Bank Statements, paying in books, cheque books	Last completed audit year	Audit
Insurance company names and policy numbers	Indefinite	Management
Insurance Policies	Whilst valid	
Employer's Liability Certificates	40 years from commencement/renewal	Statute
Budgets	Indefinite	
Quotations and Tenders	6 years	Limitations Act
Payroll Records	12 years	Superannuation

## EMPLOYMENT

<b>DOCUMENT</b>	<b>MINIMUM RETENTION PERIOD</b>	<b>REASON</b>
Timesheets	7 years	Personal Injury
Recruitment Documents	5 years	Management
Documents on Persons not hired	1 year	Equal Opportunities Claims
Accident or Injury at Work	7 years	Management
Personal administration (including CV's, appraisals, disciplinary records, contracts, pay awards etc)	6 years after person leaves	Statutory
Personnel Service Record (name, position, dates of employment, pay levels etc)	Indefinite	Management