Stelling Minnis Parish Council

General Data Protection

Regulation Policy

To be reviewed annually

Purpose of the policy and background to the General Data Protection Regulation

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 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. The Council is the data controller and the Clerk /RFO is the Data Protection Officer (DPO).

It is the DPO's 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. This will be included in the Job Description of the Clerk/RFO/DPO

Appointing the Clerk as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.

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 Risk Management Policy of the council.

Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the council undertaking training in data protection awareness.

Data breaches

One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation.

The DPO will conduct this with the support of the Parish Council. 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, the DPO will also have to notify those concerned directly.

It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on.

It is unacceptable for employees, volunteers and members to use IT 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 Notices

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 notice. This is a notice to inform individuals about what a council does with their personal information. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, 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 notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

Information Audit

The DPO 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

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- 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.

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, then the DPO must respond to this request within a month. The DPO 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.

- The Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection.
- 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.

Stelling Minnis Parish Council – November 2020

Inventory of Personal Data Captured, Stored and Processed by Stelling Minnis Parish Council

1. What Personal Data Do We Hold?			2. Lawful basis for holding personal data				3. Consent
To whom does it relate?	**What Data is it?**	**Including Sensitive Data?**	**What is it for?**	**Why do we have it?**	**Are we legally obliged to hold this data? NOTE: If we are legally obliged to hold it, no consent is needed.**	**Have we got a contract or privacy notice relating to the data subject?**	**If we have a contract with the data subject, does it demonstrate all necessary consents?**
Staff							
	Contract	Yes	HR	It is a contract	No	Contract	Yes
	PAYE	Yes	HR	Legislative requirement	Yes	Not required	Not applicable
	Bank details	No	HR	To pay staff salaries	No	Contract	Yes
	Pension details	N/A		Legislative requirement	Yes	Not required	Not applicable
	Leave Form	No	HR	Employment Purposes	No	Yes	Yes
	Staff Appraisals	Yes	HR	Employment	No	Yes	Yes
Councillors							
	Declarations of Interest	Yes	Democracy	legislative requirement	Yes	Not required	Not applicable
	Personal Contact Details	No	Democracy	legislative requirement	Yes	Not required	Not applicable
	Email Addresses	No	Democracy	legislative requirement	Yes	Not required	Not applicable
Contractors /Suppliers where we hold personal data of a natural person (not the data of a limited company or of another council)							
	Contact details	No	Business	Contact	No	Contract	
	Invoices	No	Business	Payment	No	Contract	Yes
	Purchase orders	No	Business	Purchasing	No	Contract	Yes
	Quotations	No	Business	Purchasing	No	Contract	Yes
	Bank Account details	No	Business	Payment	No	Contract	Yes
	Insurance	No	Business	Contract	No	Contract	Yes
	References	No	Business	Contact	No	Contract	Yes

Residents							
	Electoral Register	Yes	Democracy	Democracy	No	Not applicable	No contract
	Complaints	Sometimes	Democracy	Democracy	No	Privacy Notice	No contract
	Freedom of Information requests	Yes	Democracy	Democracy	Yes	Privacy Notice	No contract
	General Correspondence from MOPs	Perhaps	Democracy	Democracy	No	Privacy Notice	No contract
Community Organisations							
	Email Addresses	No	Democracy	Contact	No	Privacy Notice	No contract
	Grant Application Forms	Perhaps	Democracy	Service to community	No	Privacy Notice	No contract
	Nominations of external committee members	No	Democracy	Contact	No	Privacy Notice	No contract
Planning							
	Objections	No	Democracy	We are consulted on applications	Yes	Public Document	No contract
Property							
	Deeds for land owned	No	Property	Council function	No	Public Document	Yes
Village Hall	(We are Custodian Trustee)						
\	legal Agreements	No	Property Records	Recreation function	No	Contract	Yes
	Deeds - Land purchase	No	Property Records	Property Records	No	No	Public document
	Lease for Village Hall	No	Property Records	Property Records	No	Contract	Yes
General Contacts							
	Email Addresses	Yes	Democracy	Contact	Yes	Privacy Notice	Not applicable

Inventory assembled on 3rd April 2018

4. Sharing Personal Data	5. Our internal processes				
With whom do we share this data?	**Who is responsible for keeping this data?**	**How often is it checked?**	**How long do we keep it?**	**Where is it held?**	**Protection?**
External Professional Advisers	Clerk	On appointment and on review	Duration of Employment plus 6 years	Laptop/filing Cabinet	Password/ Lock & key
External Professional Advisers; HMRC; payroll company	Clerk	Monthly	Duration of Employment plus 6 years	Laptop/filing Cabinet	Password/ Lock & key
Our Bank; Payroll company	Clerk	Duration of Employment	Duration of Employment plus 6 years	Laptop/filing Cabinet	Password/ Lock & key
External Professional Advisers; payroll company; Pension Fund Managers; HMRC	Clerk	Duration of Employment	Duration of Employment plus 6 years	Laptop/filing Cabinet	Password/ Lock & key
External Professional Advisers	Clerk	Yearly	Duration of Employment plus 6 years	Laptop/filing Cabinet	Password/ Lock & key
	Clerk/Chairman/Vice Chairman	As required	duration of employment	Filing cabinet	lock and key
This is Public Knowledge	Clerk	At Election	Term of Office plus 4 years	Laptop/filing Cabinet	Password/ Lock & key
This is Public Knowledge	Clerk	At Election	Term of Office plus 4 years	Laptop/filing Cabinet	Password/ Lock & key
This is Public Knowledge	Clerk	At Election	Term of Office plus 4 years	Laptop/filing Cabinet	Password/ Lock & key
External Professional Advisers	Clerk	When Appointed	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Public inspection on audit	Responsible Finance Officer	On raising	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Public inspection on audit	Responsible Finance Officer	On raising	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Public inspection on audit	Responsible Finance Officer	On raising	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Our bank	Responsible Finance Officer	On raising	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
External professional advisers	Responsible Finance Officer	On appointment	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
External professional advisers	Responsible Finance Officer	On appointment	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key

Public Document required by law, which we choose to hold.	Clerk	On receipt	1 Year	Laptop/filing Cabinet	None required
External Professional Advisers, MPs, principal councils.	Clerk	On receipt	1 year	Laptop/filing Cabinet	Password/ Lock & key
External Professional Advisers	Clerk	On receipt	2 years	Laptop/filing Cabinet	Password/ Lock & key
External Professional Advisers, MPs, principal councils.	Clerk	On receipt	1 year	Laptop/filing Cabinet	Password/ Lock & key
Nobody without consent	Clerk	On receipt	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
External Professional Advisers	Clerk	On receipt	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Names become Public Knowledge, other data is confidential	Clerk	Annually	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Our objection or approval is a public document	Clerk	On receipt	1 year	Laptop/filing Cabinet	None required
Public Document registered at Land Registry	Clerk	Annually	Indefinitely	Laptop/filing Cabinet	Password/ Lock & key
Public Document registered at Land Registry	Clerk	Annually	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Public Document registered at Land Registry	Clerk	Annually	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
Public Document registered at Land Registry	Clerk	Annually	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key
	Clerk	On raising	See document Retention Policy	Laptop/filing Cabinet	Password/ Lock & key

Stelling Minnis Parish Council
Retention and Disposal Policy

1. Introduction

1.1 The Council accumulates a vast amount of information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of document.

1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.

1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.

1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the Council.

1.5 In contrast to the above the Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

2. Scope and Objectives of the Policy

2.1 The aim of this document is to provide a working framework to determine which documents are:

- Retained – and for how long; or
- Disposed of – and if so by what method.

2.2 There are some records that do not need to be kept at all or that are routinely destroyed in the course of business. This usually applies to information that is duplicated, unimportant or only of a short-term value. Unimportant records of information include:

- 'With compliments' slips.
- Catalogues and trade journals.
- Non-acceptance of invitations.
- Trivial electronic mail messages that are not related to Council business.
- Requests for information such as maps, plans or advertising material.
- Out of date distribution lists.

2.3 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed.

2.4 Records should not be destroyed if the information can be used as evidence to prove that something has happened. If destroyed the disposal needs to be disposed of under the General Data Protection Regulations.

3. Roles and Responsibilities for Document Retention and Disposal

3.1 Councils are responsible for determining whether to retain or dispose of documents and should undertake a review of documentation at least on an annual basis to ensure that any unnecessary documentation being held is disposed of under the General Data Protection Regulations.

3.2 Councils should ensure that all employees are aware of the retention/disposal schedule.

4. Document Retention Protocol

4.1 Councils should have in place an adequate system for documenting the activities of their service. This system should take into account the legislative and regulatory environments to which they work.

4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:

- Facilitate an audit or examination of the business by anyone so authorised.
- Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.
- Verify individual consent to record, manage and record disposal of their personal data.
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

4.3 To facilitate this the following principles should be adopted:

- Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations
- Documents that are no longer required for operational purposes but need retaining should be placed at the records office.

4.4 The retention schedules in Appendix A: List of Documents for Retention or Disposal provide guidance on the recommended minimum retention periods for specific classes of documents and records. These schedules have been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.

4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

5. Document Disposal Protocol

5.1 Documents should only be disposed of if reviewed in accordance with the following:

- Is retention required to fulfil statutory or other regulatory requirements?
- Is retention required to meet the operational needs of the service?
- Is retention required to evidence events in the case of dispute?
- Is retention required because the document or record is of historic interest or intrinsic value?

5.2 When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the General Data Protection Regulations.

5.3 Documents can be disposed of by any of the following methods:

- Non-confidential records: place in waste paper bin for disposal.
- Confidential records or records giving personal information: shred documents.
- Deletion of computer records.
- Transmission of records to an external body such as the County Records Office.

5.4 The following principles should be followed when disposing of records:

- All records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the Council being prosecuted under the General Data Protection Regulations.
- The Freedom of Information Act or cause reputational damage.
- Where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner.
- Where documents are of historical interest it may be appropriate that they are transmitted to the County Records office.
- Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).

5.5 Records should be maintained of appropriate disposals. These records should contain the following information:

- The name of the document destroyed.
- The date the document was destroyed.
- The method of disposal.

6. Data Protection Act 1998 – Obligation to Dispose of Certain Data

6.1 The Data Protection Act 1998 ('Fifth Principle') requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. Section 1 of the Data Protection Act defines personal information as:

> Data that relates to a living individual who can be identified:
> a) from the data, or
> b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.
>
> It includes any expression of opinion about the individual and any indication of the intentions of the Council or other person in respect of the individual.

6.2 The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely provided that the specific requirements are met.

6.3 Councils are responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations namely:

- Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal data shall only be obtained for specific purposes and processed in a compatible manner.
- Personal data shall be adequate, relevant, but not excessive.
- Personal data shall be accurate and up to date.
- Personal data shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of the data subject.
- Personal data shall be kept secure.

6.4 External storage providers or archivists that are holding Council documents must also comply with the above principles of the General Data Protection Regulations.

7. Scanning of Documents

7.1 In general once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs.

7.2 As a general rule hard copies of scanned documents should be retained for three months after scanning.

7.3 Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs.

8. Review of Document Retention

8.1 It is planned to review, update and where appropriate amend this document on a regular basis (at least every three years in accordance with the *Code of Practice on the Management of Records* issued by the Lord Chancellor).

8.2 This document has been compiled from various sources of recommended best practice and with reference to the following documents and publications:

- *Local Council Administration*, Charles Arnold-Baker, 910^{h} edition, Chapter 11
- Local Government Act 1972, sections 225 – 229, section 234
- SLCC Advice Note 316 Retaining Important Documents
- SLCC Clerks' Manual: Storing Books and Documents
- *Lord Chancellor's Code of Practice on the Management of Records* issued under Section 46 of the *Freedom of Information Act 2000*

9. List of Documents

9.1 The full list of the Council's documents and the procedures for retention or disposal can be found in Appendix A: List of Documents for Retention and Disposal. This is updated regularly in accordance with any changes to legal requirements.

Stelling Minnis Parish Council Appendix A: List of Documents for Retention or Disposal

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Minutes	Indefinite	Archive	Clerks Home Office	Original signed paper copies of Council minutes of meetings must be kept indefinitely in safe storage. At regular intervals of not more than 5 years they must be archived and deposited with the Higher Authority
Agendas	5 years	Management	Clerks Home Office	Bin (shred confidential waste)
Accident/incident reports	20 years	Potential claims	Clerks Home Office	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Scales of fees and charges	6 years	Management	Clerks Home Office	Bin
Receipt and payment accounts	Indefinite	Archive	Clerks Home Office	N/A
Receipt books of all kinds	6 years	VAT	Clerks Home Office	Bin
Bank statements including deposit/savings accounts	Last completed audit year	Audit	Clerks Home Office	Confidential waste
Bank paying-in books	Last completed audit year	Audit	Clerks Home Office	Confidential waste
Cheque book stubs	Last completed audit year	Audit	Clerks Home Office	Confidential waste
Quotations and tenders	6 years	Limitation Act 1980 (as amended)	Clerks Home Office	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Paid invoices	6 years	VAT	Clerks Home Office	Confidential waste

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Paid cheques	6 years	Limitation Act 1980 (as amended)	Clerks Home Office	Confidential waste
VAT records	6 years generally but 20 years for VAT on rents	VAT	Clerks Home Office	Confidential waste
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)	Clerks Home Office	Confidential waste
Wages books/payroll	12 years	Superannuation	Clerks Home Office	Confidential waste
Insurance policies	While valid (but see next two items below)	Management	Clerks Home Office	Bin
Insurance company names and policy numbers	Indefinite	Management	Clerks Home Office	N/A
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 (SI 2753) Management	Clerks Home Office	Bin
Investments	Indefinite	Audit, Management	Clerks Home Office	N/A
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management	Clerks Home Office	N/A
Members' allowances register	6 years	Tax, Limitation Act 1980 (as amended)	Clerks Home Office	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Information from other bodies e.g. circulars from county associations, NALC, principal authorities	Retained for as long as it is useful and relevant		Clerks Home Office	Bin
Local/historical information	Indefinite – to be securely kept for benefit of the Parish	Councils may acquire records of local interest and accept gifts or records of general and local	Stelling Minnis Village Hall	N/A

Document	Minimum Retention Period	Reason	Location Retained	Disposal
		interest in order to promote the use for such records (defined as materials in written or other form setting out facts or events or otherwise recording information).		
Magazines and journals	Council may wish to keep its own publications For others retain for as long as they are useful and relevant.	The Legal Deposit Libraries Act 2003 (the 2003 Act) requires a local council which after 1st February 2004 has published works in print (this includes a pamphlet, magazine or newspaper, a map, plan, chart or table) to deliver, at its own expense, a copy of them to the British Library Board (which manages and controls the British Library). Printed works as defined by the 2003 Act published by a local council therefore constitute materials which the British Library holds.	Clerks Home Office	Bin if applicable
Record-keeping				
To ensure records are easily accessible it is necessary to comply with the following:	The electronic files will be backed up periodically on a portable hard.	Management	Clerks Home Office	Documentation no longer required will be disposed of, ensuring any

Document	Minimum Retention Period	Reason	Location Retained	Disposal
• A list of files stored in cabinets will be kept • Electronic files will be saved using relevant file names				confidential documents are destroyed as confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
General correspondence	Unless it relates to specific categories outlined in the policy, correspondence, both paper and electronic, should be kept. Records should be kept for as long as they are needed for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests.	Management	Clerks Home Office	Bin (shred confidential waste) A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Correspondence relating to staff	If related to Audit, see relevant sections above. Should be kept securely and personal data in relation to staff should not be kept for longer than is necessary for the purpose it was held. Likely time limits for tribunal claims between 3–6 months Recommend this period be for 3 years	After an employment relationship has ended, a council may need to retain and access staff records for former staff for the purpose of giving references, payment of tax, national insurance contributions and pensions, and in respect of any related legal claims made against the council.	Clerks Home Office	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Documents from legal matters, negligence and other torts Most legal proceedings are governed by the Limitation Act 1980 (as amended). The 1980 Act provides that legal claims may not be commenced after a specified period. Where the limitation periods are longer than other periods specified the documentation should be kept for the longer period specified. Some types of legal proceedings may fall within two or more categories. If in doubt, keep for the longest of the three limitation periods.				
Negligence	6 years		Clerks Home Office	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Defamation	1 year		Clerks Home Office	Clerks Home Office
Contract	6 years		Clerks Home Office	Clerks Home Office
Leases	12 years		Clerks Home Office	Clerks Home Office
Sums recoverable by statute	6 years		Clerks Home Office	Clerks Home Office
Personal injury	3 years		Clerks Home Office	Clerks Home Office
To recover land	12 years		Clerks Home Office	Clerks Home Office
Rent	6 years		Clerks Home Office	Clerks Home Office
Breach of trust	None		Clerks Home Office	Clerks Home Office

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Planning Papers				
Applications	1 year	Management	Clerks Home Office	Clerks Home Office
Appeals	1 year unless significant development	Management	Clerks Home Office	Clerks Home Office
Trees	1 year	Management	Clerks Home Office	Clerks Home Office
Local Development Plans	Retained as long as in force	Reference	Clerks Home Office	Clerks Home Office
Local Plans	Retained as long as in force	Reference	Clerks Home Office	Clerks Home Office
Town/Neighbourhood Plans	Indefinite – final adopted plans	Historical purposes	Clerks Home Office	Clerks Home Office

Stelling Minnis Parish Council

Data Security Breach Reporting Form

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is Stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, Hacking attack, 'Blagging' offences where information is obtained by deceiving the organisation who holds it. Use this form to report such breaches.

Example: Reportable Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using the below link:

https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

Breach Containment and Recovery

Article 2(2) of the Notification Regulation states:

The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

Date and time of Notification of Breach	
Notification of Breach to whom Name Contact Details	
Details of Breach	

Nature and content of Data Involved	
Number of individuals affected:	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner informed Time and method of contact https://report.ico.org.uk/security-breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals?	

Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	

Evaluation and response	

Stelling Minnis Parish Council

Privacy Impact Assessment

As part of the PIA process organisations should describe how information is collected, stored, used and deleted.

Project Name	

What is the Projects Outcome	
Information to be obtained	
What is the information to be used for?	
Who will obtain it?	
Who will have access to the information?	
Any other Information?	
Identify Possible Privacy Risks Risks to individuals, Corporate Risks, Compliance Risks, Associated Organisation/Corporate Risk	
Identify how to mitigate these Risks Risk, Solution, Result and Evaluation.	
Evaluate costs involved	
Recourses required for the project	
Review Process Who will action the review? When will it be reviewed? Action to be take Date for completion Responsibility for action. Lessons learnt	

What to think about when preparing the Privacy Impact Assessment.
This form is to be used in conjunction with Conducting Privacy Impact Assessments Code of Practice.

It can be integrated with consultation or planning processes. Effective consultation internally within the Council is an important part of any Privacy Impact Assessment (PIA) .PIA. Data protection risks are more likely to remain unmitigated on projects which have not involved discussions with the people building a system or carrying out procedures.

Screening questions to help you decide whether a Privacy Impact Assessment is required:
Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to Organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

Will the project require you to contact individuals in ways which they may find intrusive?

When preparing your Privacy Impact Assessment you need to identify the below possible Stake holders.

- Project management team
  The team responsible for the overall implementation of a project will play a central role in the PIA process.

- Data protection officer
  If an organisation has a dedicated DPO, they are likely to have a close link to a PIA. Even if project managers are responsible for individual PIAs, the DPO will be able to provide specialist knowledge on privacy issues,

- Engineers, developers and designers
  The people who will be building a product need to have a clear understanding of how to approach privacy issues. They will also be able to suggest workable privacy solutions to the risks which have been identified.

- Information technology (IT)
  Will be able to advise on security risks and solutions. The role of IT is limited to security, and might also include discussions on the usability of any software.

- Procurement
  If the project will require systems or services to be procured, the needs of the project need to be established before procurement takes place.

- Potential suppliers and data processors
  If some of the project will be outsourced to a third party, early engagement will help to understand which options are available.

- Communications
  A PIA can become a useful part of a project's communication strategy. For example, involving communications colleagues in the PIA can help to establish a clear message to the public about a project.

- Customer-facing roles
  It is important to consult with the people who will have to use a new system or put a policy into practice. They will be able to advise on whether the system will work as intended.

- Corporate governance/compliance
  Colleagues who work on risk management for an organisation should be able to integrate PIAs into their work. Other areas of compliance can be included in the PIA process.

- Researchers, analysts, and statisticians
  Information gathered by a new project may be used to analysing customer behaviour or for other statistical purposes. Where relevant, consulting with researchers can lead to more effective safeguards such as anonymisation.

- Senior management
  It will be important to involve those with responsibility for signing off or approving a project.

External Consultation

External consultation means seeking the views of the people who will be affected by the project. This may be members of the public, but can also mean people within an organisation (for example staff who will be affected by a new online HR system). Consultation with the people who will be affected is an important part of the PIA process. There are two main aims. Firstly, it enables an organisation to understand the concerns of those individuals. The consultation will also improve transparency by making people aware of how information about them is being used.

A thorough assessment of privacy risks is only possible if an organisation fully understands how information is being used in a project. An incomplete understanding of how information is used can be a significant privacy risk – for example; data might be used for unfair purposes, or disclosed inappropriately.

You must have regard when linking to the Privacy Impact Assessment to the 8 Data Protection principals below:

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will individuals be told about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the information you are using of good enough quality for the purposes it is used for?

Which personal data could you not use, without compromising the needs of the project?

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Councillor Privacy Notice
Stelling Minnis Parish Council

The information you provide (personal information such as name, address, email address, phone number, register of interests and other relevant information) will be processed and stored so that it is possible to contact you, respond to your correspondence and retain information relating to your time in office with the Council.

The Council ask that you provide a dedicated email address for conducting Council business.

Your personal information will not be shared with any third party other than those related to a statutory or lawful requirement or with your consent.

When you contact us
The information you provide (personal information such as name, address, email address, phone number, organisation) will be processed and stored to enable us to contact you and respond to your correspondence, provide information and/or access our facilities and services. Your personal information will be not shared or provided to any other third party.

The Councils Right to Process Information
General Data Protection Regulations Article 6 (1) (a) (b) and (e)

Processing is with consent of the data subject or
Processing is necessary for compliance with a legal obligation or
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Information Security
Stelling Minnis Parish Council has a duty to ensure the security of personal data.
We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies.
Copies of these policies can be requested.

We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted. (You many request the deletion of your data held by Stelling Minnis Parish Council at any time).

Access to Information
You have the right to request access to the information we have on you. You can do this by contacting our Data Information Officer

Information Correction
If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact the Parish Clerk to request this.

Information Deletion
If you wish Stelling Minnis Parish Council to delete the information about you please contact the Parish Clerk to request this.

Right to Object
If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact the DPO to object.

Rights Related to Automated Decision Making and Profiling
Stelling Minnis Parish Council does not use any form of automated decision making or the profiling of individual personal data.

Complaints
If you have a complaint regarding the way your personal data has been processed you may make a complaint to Stelling Minnis PC Data Information Officer or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Summary: In accordance with the law:

Stelling Minnis Parish Council only collect a limited amount of information about you that is necessary for correspondence, information and service provision.

Stelling Minnis Parish Council do not use profiling, we do not sell or pass your data to third parties.

Stelling Minnis Parish Council do not use your data for purposes other than those specified.

Stelling Minnis Parish Council make sure your data is stored securely.

Stelling Minnis Parish Council delete all information deemed to be no longer necessary.

Stelling Minnis Parish Council constantly review our Privacy Policies to keep it up to date in protecting your data.

(You can request a copy of our policies at any time).

Stelling Minnis Parish Council
General Data Protection Regulations (Service) Consent
to hold Contact Information

I agree that I have read and understand Stelling Minnis Parish Councils Privacy Notice. I agree by signing below that the Council may process my personal information for providing information and corresponding with me.

I agree that Stelling Minnis Parish Council can keep my contact information data for an undisclosed time or until I request its removal.

I have the right to request modification on the information that you keep on record.

I have the right to withdraw my consent and request that my details are removed from your database.

Name	
Date of birth if under 18	
Parental/Guardian Consent for any data processing activity	
Address	
Telephone No.	
Email Address	
Facebook	
Twitter	
Signature	
Date	

For office use only:

Guidance Notes Data Sharing Checklist – systematic data sharing
Scenario: You want to enter into an agreement to share personal data on an ongoing basis is this form relevant and the sharing justified? Read the below:

Key points to consider:
What is the sharing meant to achieve?
Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place.
As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared?
- •The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Date Data received	Date consent received and approved for data to be held	Data received as Phone, email, hard copy or other	Data approved to be shared with the below	Removal of consent received	Date data disposed of and method of disposal actioned

Stelling Minnis Parish Council
Email Contact Privacy Notice

When you contact us
The information you provide (personal information such as name, address, email address, phone number, organisation) will be processed and stored to enable us to contact you and respond to your correspondence, provide information and/or access our facilities and services. Your personal information will be not shared or provided to any other third party.

The Councils Right to Process Information
General Data Protection Regulations Article 6 (1) (a) (b) and (e)

Processing is with consent of the data subject or
Processing is necessary for compliance with a legal obligation or
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Information Security
Stelling Minnis Parish Council has a duty to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. Copies of these policies can be requested.

We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted. (You many request the deletion of your data held by Stelling Minnis Parish Council at any time).

Children
We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Access to Information
You have the right to request access to the information we have on you. You can do this by contacting our Data Information Officer.

Information Correction
If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate.

Information Deletion
If you wish Stelling Minnis Parish Council to delete the information about you please contact the Parish Clerk to request this.

Right to Object
If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact the DPO to object.

Rights Related to Automated Decision Making and Profiling
Stelling Minnis Parish Council does not use any form of automated decision making or the profiling of individual personal data.

Complaints
If you have a complaint regarding the way your personal data has been processed you may make a complaint to Stelling Minnis Parish Council Data Information Officer and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Summary: In accordance with the law,

Stelling Minnis Parish Council only collect a limited amount of information about you that is necessary for correspondence, information and service provision.

Stelling Minnis Parish Council do not use profiling, we do not sell or pass your data to third parties.

Stelling Minnis Parish Council do not use your data for purposes other than those specified.

Stelling Minnis Parish Council make sure your data is stored securely.

Stelling Minnis Parish Council delete all information deemed to be no longer necessary.

Stelling Minnis Parish Council constantly review our Privacy Policies to keep it up to date in protecting your data. (You can request a copy of our policies at any time).

Stelling Minnis Parish Council

Social Media and Electronic Communication Policy

The use of digital and social media and electronic communication enables the Parish Council to interact in a way that improves the communications both within the Council and between the Council and the people, businesses and agencies it works with and serves.

The Council has a website and uses email to communicate. The Council will always try to use the most effective channel for its communications. Over time the Council may add to the channels of communication that it uses as it seeks to improve and expand the services it delivers. When these changes occur this Policy will be updated to reflect the new arrangements.

Communications from the Council will meet the following criteria:

- Be civil, tasteful and relevant;
- Not contain content that is knowingly unlawful, libellous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive;
- Not contain content knowingly copied from elsewhere, for which we do not own the copyright;
- Not contain any personal information.
- If it is official Council business it will be moderated by either the Chair/Vice Chair of the Council or the Clerk to the Council;
- Social media will not be used for the dissemination of any political advertising.

In order to ensure that all discussions on the Council page are productive, respectful and consistent with the Council's aims and objectives, we ask you to follow these guidelines:

- Be considerate and respectful of others. Vulgarity, threats or abuse of language will not be tolerated.
- Differing opinions and discussion of diverse ideas are encouraged, but personal attacks on anyone, including the Council members or staff, will not be permitted.
- Share freely and be generous with official Council posts, but be aware of copyright laws; be accurate and give credit where credit is due.
- Stay on topic.

The site is not monitored 24/7 and we will not always be able to reply individually to all messages or comments received. However, we will endeavour to ensure that any emerging themes or helpful suggestions are passed to the relevant people or authorities. Please do not include personal/private information in your social media posts to us.

Sending a text or instant message will not be considered as contacting the Council for official purposes and we will not be obliged to monitor or respond to requests for information through these channels. Instead, please make direct contact with the council's Clerk and/or members of the council by emailing.

We retain the right to remove comments or content that includes:

- Obscene or racist content
- Personal attacks, insults, or threatening language
- Potentially libellous statements.
- Plagiarised material; any material in violation of any laws, including copyright
- Private, personal information published without consent
- Information or links unrelated to the content of the forum
- Commercial promotions or spam
- Alleges a breach of a Council's policy or the law

The Council's response to any communication received not meeting the above criteria will be to either ignore, inform the sender of our policy or send a brief response as appropriate. This will be at the Council's discretion based on the message received, given our limited resources available.

Parish Council Website.
Where necessary, we may direct those contacting us to our website to see the required information, or we may forward their question to one of our Councillors for consideration and response. We may not respond to every comment we receive particularly if we are experiencing a heavy workload.
The Council may, at its discretion, allow and enable approved local groups to have and maintain a presence on its website for the purpose of presenting information about the group's activities. The local group would be responsible for maintaining the content and ensuring that it meets the Council's 'rules and expectation' for the web site. The Council reserves the right to remove any or all of a local group's information from the web site if it feels that the content does not meet the Council's 'rules and expectation' for its website. Where content on the website is maintained by a local group it should be clearly marked that such content is not the direct responsibility of the Council.

Parish Council email
The Clerk to the council has their own council email address: irenebowie.smpc@gmail.com

We aim to reply to all questions sent as soon as we can.

The Clerk is responsible for dealing with email received and passing on any relevant mail to members or external agencies for information and/or action. All communications on behalf of the Council will usually come from the Clerk, and/or otherwise will always be copied to the Clerk. All new Emails requiring data to be passed on, will be followed up with a Data consent form for completion before action is taken with that correspondence.

Individual Councillors are at liberty to communicate directly with parishioners in relation to their own personal views, if appropriate, copy to the Clerk.

NB any emails copied to the Clerk become official and will be subject to The Freedom of Information Act.

These procedures will ensure that a complete and proper record of all correspondence is kept.

Do not forward personal information on to other people or groups outside of the Council, this includes names, addresses, email, IP addresses and cookie identifiers.

SMS (texting)
Members and the Clerk may use SMS as a convenient way to communicate at times. All are reminded that this policy also applies to such messages.

Video Conferencing e.g. Skype
If this medium is used to communicate please note that this policy also applies to the use of video conferencing.

Internal communication and access to information within the Council
The Council is continually looking at ways to improve its working and the use of social media and electronic communications is a major factor in delivering improvement.

Councillors are expected to abide by the Code of Conduct and the Data Protection Act in all their work on behalf of the Council
As more and more information becomes available at the press of a button, it is vital that all information is treated sensitively and securely. Councillors are expected to maintain an awareness of the confidentiality of information that they have access to and not to share confidential information with anyone. Failure to properly observe confidentiality may be seen as a breach of the Council's Code of Conduct and will be dealt with through its prescribed procedures (at the extreme it may also involve a criminal investigation). Members should also be careful only to cc essential recipients on emails i.e. to avoid use of the 'Reply to All' option if at all possible, but of course copying in all who need to know and ensuring that email trails have been removed.