REPORT TO COUNCIL

Title: GENERAL DATA PROTECTION REGULATIONS
Report of: CLERK
Date: 16 May 2018

SUMMARY:
The General Data Protection Regulations (GDPR) will apply from 25th May 2018. The ICO has released a 12-point checklist of steps that we need to take to help us in our journey to become GDPR compliant - this has been previously distributed to Councillors. This report summarises the points in relation to our Council and presents new policies/procedures for approval.

REPORT:

1. Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Scaleby Parish Council, as a corporate body, is the formal Data Controller. Information is being disseminated through the Clerk and Councillors are urged to read other information, widely available through the ICO website.

The Clerk will continue to forward relevant information on both GDPR and also Cyber-Security which is a key component. A checklist is also attached (for receipt by signature) for all members (Appendix 1).

2. Information You Hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

A data audit schedule (Appendix 2) has been produced to help us record all the data we hold, why we are holding it, the legal basis for holding it, whether consent is necessary and how we should be protecting it. A risk assessment has also been compiled (Appendix 3).

3. Individuals' Rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

We have produced various policies to cover this, namely:

- General Data Protection Regulations (Service) Consent to hold Contact Information (Appendix 4);
- Document Retention and Disposal Policy (Updated document in Appendices 5 and 6);
- Information Data Protection Policy (Appendix 7);
- Removable Media Policy (Appendix 8);
- Social Media Policy (Appendix 9); and

- an updated policy on filming (Appendix 10)

4. Communicating Privacy Information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for the GDPR implementation.

We have produced various policies to cover this requirement including: (Appendix Three).

- Privacy Notice (Appendix 11);
- Email Contact Privacy Notice (Appendix 12);
- New Councillor Contact Privacy Notice (Appendix 13)
- Privacy Impact Assessment (Appendix 14)

5. Lawful Basis for Processing Personal Data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Please refer to Appendices 2 and 11.

6. Subject Access Requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

We have produced a policy to cover this (Appendix 15).

7. Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

Please refer to the documents listed under point *3 Individuals' Rights*.

8. Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

We have formulated a procedure for this (Appendix 16).

9. Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

We do not hold specific data for any children therefore we do not need to concern ourselves with this point.

10. Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

The key point here is minimising the risk to information privacy - the risk of harm through use or misuse of personal information. The ICO says that some of the ways this risk can arise are through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person is it about; or
- not kept securely.

We, as a Council, have to take full account of these requirements when adding to or reviewing our ways of working. A Data Protection Impact Assessment can be used to assist in this (Appendix 14). There is more information available online about this at the ICO website. This will need continuing work and links in with the cyber-security aspects also.

11. Data Protection Officer

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

The Government has tabled an amendment to its own Data Protection Bill to exempt all parish and town councils and parish meetings in England and community and town councils in Wales from the requirement to appoint a Data Protection Officer (DPO) under the General Data Protection Regulation.

Officials from the Department for Culture, Media and Sport have confirmed that all other measures will still apply, but that appointing a Data Protection Officer to support a council's approach to data protection will be discretionary and may be regarded as good practice.

12. International

If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

This does not apply to our Council.

ACTION:

The Council is asked to approve the necessary policies for immediate implementation and action any associated outcomes from them.

APPENDIX 1

GENERAL DATA PROTECTION AWARENESS CHECKLIST FOR COUNCILLORS

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

General Data Protection Awareness Checklist for Councillors

The General Data Protection Regulation (GDPR) will apply in the UK from 25th May. Whilst Parish Councils are expected to comply with GDPR, individual councillors will also need to ensure that they protect an individual's personal data whether it is stored electronically or as a hard copy. This applies only to living individuals (not the deceased, companies, other authorities and charities)

Personal data includes:

- Names and addresses
- Telephone numbers
- Email addresses
- IP addresses

The following measures are recommended to help councillors comply with GDPR:

Action	Noted ✓
Set up a separate email account for parish council correspondence	
Ensure that all devices (computers, laptops, phones) are password protected	
Do not forward on emails or email threads as they may contain personal data	
Copy and paste information from an email if you want to pass it on, rather than forwarding on an email to remove the IP address from the header.	
Where possible direct all correspondence to the clerk who can obtain the necessary consent	
Where possible avoid holding an individual's information in a councillor's home or on a councillor's own PC. If a councillor has to hold any information containing personal data on behalf of the Parish Council, it needs to be stored securely in a locked room or cabinet or if on a PC, in an encrypted folder.	
Make sure your antivirus software and operating system is up-to-date	
Make sure your computer's firewall is turned on	
Inform the Data Protection Officer of any breaches within 48 hours	

I confirm that I have read the information above and understand my responsibility as a parish councillor for protecting personal data.

Signed: Date:

APPENDIX 2

INVENTORY OF PERSONAL DATA CAPTURED, STORED AND PROCESSED

Inventory assembled on 13/04/2018 and Last updated on 13/4/2018

5. Our internal processes					6. Action Needed
Who is responsible for keeping this data?	**How often is it checked?**	**How long do we keep it?**	**Where is it held?**	**Protection?**	**Action needed**
Clerk	On appointment and on review	Duration of Employment plus 6 years	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Monthly	Duration of Employment plus 6 years	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Duration of Employment	Duration of Employment plus 6 years	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Duration of Employment	Duration of Employment plus 6 years	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Yearly	Duration of Employment plus 6 years	Computer/filing Cabinet	Password/ Lock & key	
Clerk	As required	duration of employment	Filing cabinet	lock and key	
Clerk	At Election	Term of Office plus 4 years	Computer/filing Cabinet	Password/ Lock & key	Comply with document retention policy
Clerk	At Election	Term of Office plus 4 years	Computer/filing Cabinet	Password/ Lock & key	
Clerk	At Election	Term of Office plus 4 years	Computer/filing Cabinet	Password/ Lock & key	Suggest stand alone email address for all councillors
Clerk	When Appointed	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	Clerk holds contact details for contractors/suppliers
Responsible Finance Officer	On raising	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Responsible Finance Officer	On raising	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Responsible Finance Officer	On raising	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Responsible Finance Officer	On raising	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Responsible Finance Officer	On appointment	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Responsible Finance Officer	On appointment	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Clerk	On receipt	1 Year	Computer/filing Cabinet	None required	
Clerk	On receipt	1 year	Computer/filing Cabinet	Password/ Lock & key	
Clerk	On receipt	2 years	Computer/filing Cabinet	Password/ Lock & key	
Clerk	On receipt	1 year	Computer/filing Cabinet	Password/ Lock & key	Ensure document retention policy complies
Clerk	On receipt	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Clerk	On receipt	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Annually	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Clerk	On receipt	1 year	Computer/filing Cabinet	None required	
Clerk	Annually	Indefinitely	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Annually	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Annually	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Clerk	Annually	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	
Clerk	On raising	See document Retention Policy	Computer/filing Cabinet	Password/ Lock & key	Comply with document retention policy

Council Profile	Small Parish Council
	Councillors 7 out of 8
	Staff 1 Clerk Part time
	Electorate TBC
	Precept 2018/2019 £5,400
	Common Land and Village Green areas
	Custodian of Village Hall

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

1. What Personal Data Do We Hold?			2. Lawful basis for holding personal data				3. Consent	4. Sharing Personal Data
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?**	**With whom do we share this data?**
Staff								
	Contract	Yes	HR	It is a contract	No	Contract	Yes	External Professional Advisers
	PAYE	No	HR	Legislative requirement	Yes	Not required	Not applicable	External Professional Advisers; HMRC; payroll company
	Bank details	No	HR	To pay staff salaries	No	Contract	Yes	Our Bank; Payroll company
	Pension details	Yes	HR	Legislative requirement	Yes	Not required	Not applicable	External Professional Advisers; payroll company; Pension Fund Managers; H
	Leave Form	No	HR	Employment Purposes	No	Yes	Yes	External Professional Advisers
	Staff Appraisals	Yes	HR	Employment	No	Yes	Yes	
Councillors								
	Declarations of Interest	Yes	Democracy	legislative requirement	Yes	Not required	Not applicable	This is Public Knowledge
	Personal Contact Details	No	Democracy	legislative requirement	Yes	Not required	Not applicable	This is Public Knowledge
	Email Addresses	No	Democracy	legislative requirement	Yes	Not required	Not applicable	This is Public Knowledge
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	Yes	External Professional Advisers
	Invoices	No	Business	Payment	No	Contract	Yes	Public inspection on audit
	Purchase orders	No	Business	Purchasing	No	Contract	Yes	Public inspection on audit
	Quotations	No	Business	Purchasing	No	Contract	Yes	Public inspection on audit
	Bank Account details	No	Business	Payment	No	Contract	Yes	Our bank
	Insurance	No	Business	Contract	No	Contract	Yes	External professional advisers
	References	No	Business	Contact	No	Contract	Yes	External professional advisers
Residents								
	Electoral Register	No	Democracy	Democracy	No	Not applicable	No contract	Public Document required by law, which we choose to hold.
	Complaints	Sometimes	Democracy	Democracy	No	Privacy Notice	No contract	External Professional Advisers, MPs, principal councils.
	Freedom of Information requests	No	Democracy	Democracy	Yes	Privacy Notice	No contract	External Professional Advisers
	General Correspondence from MOPs	Perhaps	Democracy	Democracy	No	Privacy Notice	No contract	External Professional Advisers, MPs, principal councils.
Community Organisations								
	Email Addresses	No	Democracy	Contact	No	Privacy Notice	No contract	Nobody without consent
	Grant Application Forms	Perhaps	Democracy	Service to community	No	Privacy Notice	No contract	External Professional Advisers
	Nominations of external committee members	No	Democracy	Contact	No	Privacy Notice	No contract	Names become Public Knowledge, other data is confidential
Planning								
	Objections	No	Democracy	We are consulted on applications	Yes	Public Document	No contract	Our objection or approval is a public document
Property								
	Lease for Village Green	No	Property	Council function	No	Public Document	Yes	Public Document registered at Land Registry
Village Hall	(We are Custodian Trustee)							
	legal Agreements	No	Property Records	Recreation function	No	Contract	Yes	Public Document
	Deeds - Land purchase	No	Property Records	Property Records	No	No	Public document	Public Document
	Lease for Village Hall	No	Property Records	Property Records	No	Contract	Yes	Public Document
General Contacts								
	Email Addresses	Yes	Democracy	Contact	Yes	Privacy Notice	Not applicable	Any reasonable request

APPENDIX 3

GDPR RISK ASSESSMENT

GDPR Risk Assessment

Scaleby Parish Council: **Date: 16 May 2018**

Area of risk	Risk Identified	Risk Level H/M/L	Management of Risk	Action taken/completed
All personal data	Personal data falls into hands of a third party	H	Identify what personal data our council holds. Examples include the Electoral Roll, Job applications, tenancy agreements), why it holds it and for how long, who it shares with (see separate Assessment of Personal Data held by councils)	Data audit undertaken and ongoing work remains active on it.
		H	Identify how you store personal data. Examples include paper files, databases, electronic files, laptops and portable devices such as memory sticks or portable hard drives.	Purchase new filing cabinet keys. Purchase portable hard drive or USB flash drive. Sort through filing cabinets and destroy confidential waste no longer needed. Remove emails older than 6 months/1 year if no longer required.
	Publishing of personal data in the minutes and other council documents	L	Avoid including any personal information in the minutes or other council documents which are in the public domain. Instead of naming a person, say 'a resident/member of the public unless necessary.	No details written in current format. Historical minutes do display occasionally.
Sharing of data	Personal data falls into hands of a third party	L	Does our council share personal data with any other organisations, for example other local authorities? If yes, you may need to set up a written agreement with the organisation to ensure that they protect the data once passed to them	Only share with City and County Councils and will request consent forms going forward. Confirm both authorities have procedures in place.
Hard copy data	Hard copy data falls into hands of a third party	L	Decide how much of the personal data held is necessary. Destroy personal data which is no longer needed in line with the Retention of Documents policy	Sort through filing cabinets and destroy confidential waste no longer needed.
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Clerk's own office, not shared and visits by members of the public are few. Keys for filing

				cabinet to be replaced.
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	M	Ensure that all devices are password protected	Ensure passwords are set and adequate.
		M	Make all councillors aware of the risk of theft or loss of devices and the need to take sensible measures to protect them from loss or theft	Obtain signed confirmation of "checklist" from all members
			Carry out regular back-ups of council data	Data backed up on dropbox cloud. Purchase external portable hard drive for weekly backups as a precaution.
		L	Ensure safe disposal of IT equipment and printers at the end of their life	Clerk to ensure safe disposal after cleaning system.
		L	Ensure all new IT equipment has all security measures installed before use	Use reputable supplier
Email security	Unauthorised access to council emails	L	Ensure that email accounts are password protected and that the passwords are not shared or displayed publically	Safe passwords currently used and only known by Clerk (with signed copy to be stored at Chairman's residence)
		M	Set up separate parish council email addresses for employees and councillors (recommended)	Obtain signed confirmation of "checklist" from all members recommending this action
		L	Use blind copy (bcc) to send group emails to people outside the council	To implement
		M	Use encryption for emails that contain personal information	To investigate
		L	Use cut and paste into a new email to remove the IP address from the header	To implement
		L	Do not forward on emails from members of the public. If necessary copy and paste information into a new email with personal information removed.	To implement
		H	Delete emails from members of public when query has been dealt with and there is no need to keep it	Time constraints limit. Also, when does the need pass?
General internet security	Unauthorised access to council computers and files	M	Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publically	Obtain signed confirmation of "checklist" from all members recommending this action
		H	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	Obtain signed confirmation of "checklist" from all members
		M	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	
		H	Password protect personal and sensitive information folders and databases.	To implement

			Ensure that shared drives do not provide unauthorised access to HR and other records containing personal information	
Website security	Personal information or photographs of individuals published on the website	L	Ensure that you have the written consent of the individual including parental consent if the subject is 17 or under) Ensure you have a Vetting and Barring Policy	Rarely an issue No policy - investigate
Disposal of computers and printers	Data falls into the hands of a third party	L	Wipe the hard drives from computers, laptops and printers or destroy them before disposing of the device	Clerk to action
Financial Risks	Financial loss following a data breach as a result of prosecution or fines	L	Ensure that the council has liability cover which specifically covers prosecutions resulting from a data breach and put aside sufficient funds (up to 4% of income) should the council be fined for a data breach	Clerk to confirm
	Budget for GDPR and Data Protection	H	Ensure the Council has sufficient funds to meet the requirements of the new regulations both for equipment and data security and add to budget headings for the future	Budget needs to be allocated
General risks	Loss of third party data due to lack of understanding of the risks/need to protect it	M	Ensure that all staff and councillors have received adequate training and are aware of the risks	Obtain signed confirmation of "checklist" from all members
	Filming and recording at meetings	L	If a meeting is closed to discuss confidential information (for example salaries, or disciplinary matters), ensure that no phones or recording devices have been left in a room by a member of the public	Rarely an issue

Reviewed on: _____ **Signed:** _____ **(Chairman)**

APPENDIX 4

GENERAL DATA PROTECTION REGULATIONS (SERVICE) CONSENT TO HOLD CONTACT INFORMATION

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

General Data Protection Regulations (Service) Consent to hold Contact Information

I agree that I have read and understand Scaleby Parish Council's 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 Scaleby 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

APPENDIX 5

RETENTION AND DISPOSAL

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

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.

APPENDIX 6

LIST OF DOCUMENTS FOR RETENTION OR DISPOSAL

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

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Minutes	Indefinite	Archive	Current and recent years retained at Clerk's office. Older minutes at Archive Offices.	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	Clerk's office filing cabinet	Bin (shred confidential waste)
Accident/incident reports	20 years	Potential claims	Clerk's office filing cabinet	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	Clerk's office filing cabinet	Bin
Receipt and payment accounts	Indefinite	Archive	Clerk's office filing cabinet	N/A
Receipt books of all kinds	6 years	VAT	Clerk's office filing cabinet	Bin

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Bank statements including deposit/savings accounts	Last completed audit year	Audit	Clerk's office filing cabinet	Confidential waste
Bank paying-in books	Last completed audit year	Audit	Clerk's office filing cabinet	Confidential waste
Cheque book stubs	Last completed audit year	Audit	Clerk's office filing cabinet	Confidential waste
Quotations and tenders	6 years	Limitation Act 1980 (as amended)	Clerk's office filing cabinet	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	Clerk's office filing cabinet	Confidential waste
Paid cheques	6 years	Limitation Act 1980 (as amended)	Clerk's office filing cabinet	Confidential waste
VAT records	6 years generally but 20 years for VAT on rents	VAT	Clerk's office filing cabinet	Confidential waste
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)	Clerk's office filing cabinet	Confidential waste
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)	Clerk's office filing cabinet	Bin
Wages books/payroll	12 years	Superannuation	Clerk's office filing cabinet	Confidential waste
Insurance policies	While valid (but see next two items below)	Management	Clerk's office filing cabinet	Bin
Insurance company names and policy numbers	Indefinite	Management	Clerk's office filing cabinet	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	Clerk's office filing cabinet	Bin

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Play area equipment inspection reports	21 years		Clerk's office filing cabinet	
Investments	Indefinite	Audit, Management	Clerk's office filing cabinet	N/A
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management	Clerk's office filing cabinet	N/A
Members' allowances register	6 years	Tax, Limitation Act 1980 (as amended)	Clerk's office filing cabinet	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		Clerk's office filing cabinet	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 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).	Clerk's office filing cabinet	N/A

Document	Minimum Retention Period	Reason	Location Retained	Disposal
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.	Clerk's office	Bin if applicable
	Record-keeping			
To ensure records are easily accessible it is necessary to comply with the following: • A list of files stored in cabinets will be kept • Electronic files will be saved using relevant file names	The electronic files will be backed up periodically on a portable hard drive and also in a cloud-based programme	Management		Documentation no longer required will be disposed of, ensuring any 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.

Document	Minimum Retention Period	Reason	Location Retained	Disposal
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	Clerk's office filing cabinet	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.	Clerk's office filing cabinet	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		Clerk's office filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Defamation	1 year		Clerk's office filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Contract	6 years		Clerk's office filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Leases	12 years		Clerk's office filing cabinet	Confidential waste.
Sums recoverable by statute	6 years		Clerk's office filing cabinet	Confidential waste.
Personal injury	3 years		Clerk's office filing cabinet	Confidential waste.
To recover land	12 years		Clerk's office filing cabinet	Confidential waste.
Rent	6 years		Clerk's office filing cabinet	Confidential waste.
Breach of trust	None		Clerk's office filing cabinet	Confidential waste.

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Trust deeds	Indefinite		Clerk's office filing cabinet	N/A
For Halls, Centres, Recreation Grounds where applicable				
• Application to hire • Invoices • Record of tickets issued	6 years	VAT	Clerk's office filing cabinet/archive boxes	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Lettings diaries	Electronic files linked to accounts	VAT	n/a	N/A
Terms and Conditions	6 years	Management	Clerk's office filing cabinet/archive boxes	Bin
Event Monitoring Forms	6 years unless required for claims, insurance or legal purposes	Management	Clerk's office filing cabinet/archive boxes	Bin. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
	For Allotments			
Register and plans	Indefinite	Audit, Management	n/a	N/A
Minutes	Indefinite	Audit, Management	n/a	N/A
Legal papers	Indefinite	Audit, Management	n/a	N/A
	For Burial Grounds			

Document	Minimum Retention Period	Reason	Location Retained	Disposal
• Register of fees collected • Register of burials • Register of purchased graves • Register/plan of grave spaces • Register of memorials • Applications for interment • Applications for right to erect memorials • Disposal certificates • Copy certificates of grant of exclusive right of burial	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI 204)	n/a	N/A
	Planning Papers			
Applications	1 year	Management	Clerk's office filing cabinet/archive boxes	Bin
Appeals	1 year unless significant development	Management	Clerk's office filing cabinet/archive boxes	Bin
Trees	1 year	Management	Clerk's office filing cabinet/archive boxes	Bin
Local Development Plans	Retained as long as in force	Reference	Clerk's office filing cabinet/archive boxes	Bin
Local Plans	Retained as long as in force	Reference	Clerk's office filing cabinet/archive boxes	Bin
Town/Neighbourhood Plans	Indefinite – final adopted plans	Historical purposes	Clerk's office filing cabinet/archive	N/A

Document	Minimum Retention Period	Reason	Location Retained	Disposal
			boxes	
	CCTV			
Daily notes	Daily	Data protection	n/a	Confidential waste
Radio rotas	1 week	Management	n/a	Confidential waste
Work rotas	1 month	Management	n/a	Confidential waste
Observation sheets	3 years	Data protection	n/a	Confidential waste
Stats	3 years	Data protection	n/a	Confidential waste
Signing in sheets	3 years	Management	n/a	Confidential waste
Review requests	3 years	Data protection	n/a	Confidential waste
Discs – master and working	For as long as required	Data protection	n/a	Confidential waste
Internal Operations Procedure Manual	Destroy on renewal Review annually	Management	n/a	Confidential waste
Code of Practice	Destroy on renewal Review annually	Management	n/a	Confidential waste
Photographs/digital prints	31 days	Data protection	n/a	Confidential waste

APPENDIX 7

INFORMATION AND DATA PROTECTION POLICY

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

Information & Data Protection Policy

Introduction

In order to conduct its business, services and duties, Scaleby Parish Council processes a wide range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

Scaleby Parish Council will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

This Policy is linked to our ICT Policy, Removable Media Policy and Social Media Policies and will ensure information considerations are central to the ethos of the organisation.

The Parish Council will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioners Office.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Parish communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information

Scaleby Parish Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The General Data Protection Regulation (GDPR) which become law on 25th May 2018 and will like the the Data Protection Act 1998 before them, seek to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Parish Council with legitimate reasons for using personal information.

The policy is based on the premise that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Terminology

Data subject - means the person whose personal data is being processed.
That may be an employee, prospective employee, associate or prospective associate of BTC or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.
It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Parish Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.

Scaleby Parish Council processes **personal data** in order to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law;
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law;
- monitor its activities including the equality and diversity of its activities;
- fulfil its duties in operating the business premises including security (where applicable);
- assist regulatory and law enforcement agencies;
- process information including the recording and updating details about its Councillors, employees, partners and volunteers;
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint;
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council;
- undertake research, audit and quality improvement work to fulfil its objects and purposes; and
- carry out Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time.

The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract or agreement with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any **sensitive personal information** and the Parish Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?

The Parish Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Parish Clerk.

- Email: clerk@Scaleby.org.uk
- Phone: 01228 231124
- Correspondence: The Parish Clerk, Hill House, Walton, Brampton, CA8 DY

Diversity Monitoring

Scaleby Parish Council monitors the diversity of its employees, and Councillors, in order to ensure that there is no inappropriate or unlawful discrimination in the way it conducts its activities. It undertakes similar data handling in respect of prospective employees. This data will always be treated as confidential. It will only be accessed by authorised individuals within the Council and will not be disclosed to any other bodies or individuals. Diversity information will never be used as selection criteria

and will not be made available to others involved in the recruitment process. Anonymised data derived from diversity monitoring will be used for monitoring purposes and may be published and passed to other bodies.

The Council will always give guidance on personnel data to employees, councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Appropriate technical and organisational measures will be taken against Unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information provided to us
The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with Scaleby Parish Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however where ever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Parish Council is able to keep their personal data accurate and up-to-date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

The Councils Right to Process Information
General Data Protection Regulations (and Data Protection Act) 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.
Processing is necessary for the legitimate interests of the Council.

Information Security
The Parish Council cares 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.
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.

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

Rights of a Data Subject

Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting our Parish Clerk or Data Protection Officer:

Information Correction: If they believe that the information we have about them is incorrect, they may contact us so that we can update it and keep their data accurate. Please contact: Parish Clerk.

Information Deletion: If the individual wishes the Parish Council to delete the information about them, they can do so by contacting the Parish Clerk.

Right to Object: If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Parish Clerk or Data Protection Officer.

The Parish Council does not use automated decision making or profiling of individual personal data.

Complaints: If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Parish Clerk, Data Protection Officer or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

The Council will always give guidance on personnel data to employees through the Employee handbook.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making Information Available

The Publication Scheme is a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, the Website and sent to the local media. The Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each Council and committee meeting. Details can be seen in the Council's Standing Orders, which are available on its Website or at its Offices.

Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Council, but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of council and committee meetings normally open to the public. The Council will where possible facilitate such recording unless it is being

disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Disclosure Information
The Council will as necessary undertake checks on both staff and Members with the the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

Data Transparency
The Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

"Public data" means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Council's decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:
Demand led: new technologies and publication of data should support transparency and accountability
Open: the provision of public data will be integral to the Council's engagement with residents so that it drives accountability to them.
Timely: data will be published as soon as possible following production.

Government has also issued a further Code of Recommended Practice on Transparency, compliance of which is compulsory for parish councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. Scaleby Parish Council exceeds this turnover but will never the less ensure the following information is published on its Website for ease of access:

- All transactions above £100.
- End of year accounts
- Annual Governance Statements
- Internal Audit Reports
- List of Councillor or Member responsibilities
- Details of public land and building assets
- Draft minutes of Council and committees within one month
- Agendas and associated papers no later than three clear days before the meeting.

Adopted by Council: Scaleby Parish Council 16 May 2018
Review Date: 15 May 2019

APPENDIX 8

THE MANAGEMENT OF TRANSFERABLE DATA POLICY/REMOVABLE DATA POLICY

The Management of Transferable Data Policy

Contents

Purpose

1.1 This policy supports the controlled storage and transfer of information by Councillors and all employees, temporary staff and agents (contractors, consultants and others working on behalf of the Council) who have access to and use of computing equipment that is owned or leased by Hethersgill Parish Council.

1.2 Information is used throughout the Council and is sometimes shared with external organisations and applicants. The use of removable media may result in the loss of the ability to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide services to the public.

1.3 It is therefore essential for the continued operation of the Council that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Council's needs.

1.4 The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:

1.4.1 Enabling the correct data to be made available where it is required
1.4.2 Maintaining the integrity of the data
1.4.3 Preventing unintended consequences to the stability of the computer network
1.4.4 Building confidence and trust in data that is being shared between systems
1.4.5 Maintaining high standards of care towards data and information about individual parishioners, staff or information that is exempt from disclosure
1.4.6 Compliance with legislation, policies or good practice requirements

2 Principals

2.1 This policy sets out the principles that will be adopted by the Council in order for material to be safely stored on removable media so that the risk of loss or corruption to work data is low.

2.2 Removable media includes but is not limited to:
USB memory sticks, memory cards, portable memory devices, CD / DVDs, diskettes and any other device that transfers data between systems, or stores electronic data separately from email or other applications.

2.4 Any person who intends to store Council data on removable media must abide by this Policy. This requirement devolves to Councillors, employees and agents of the Council, who may be held personally liable for any breach of the requirements of this policy.

2.5 Failure to comply with this policy could result in disciplinary action.

3 Advice and Assistance

3.1 The Clerk will ensure that everyone that is authorised to access the Councils information systems is aware of their obligations arising from this policy.

3.2 A competent person should be consulted over any hardware or system issues. Advice and guidance on using software packages should be also sort from a competent person.

4 Responsibilities

4.1 Clerks are responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Council business.

4.2 Users of removable media must have adequate Records Management / Information Security training so that relevant policies are implemented.

5 Incident Management

5.1 It is the duty of all employees and agents of the Council to not allow storage media to be compromised in any way whist in their care or under their control. There must be immediate reporting of any misuse or irresponsible actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security to the Clerk.

5.2 It is the duty of all Councillors/Employees to report any actual or suspected breaches in information security to the Clerk.

6 Data Administration

6.1 Removable media should not be the only place where data created or obtained for work purposes is held, as data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up.

6.2 Where removable media is used to transfer material between systems then copies of the data should also remain on the source system or computer, until the data is successfully transferred to another computer or system.

6.3 Where there is a business requirement to distribute information to third parties, then removable media must only be used when the file cannot be sent or is too large to be sent by email or other secure electronic means.

6.4 Transferring material to removable media is a snapshot of the data at the time it was saved to the media. Adequate labelling must be undertaken so as to easily identify the version of the data, as well as its content.

6.5 Files must be deleted from removable media, or the removable media destroyed, when the operational use of the material has been completed. The Council's retention and

disposition schedule must be implemented by Councillors, employees, contractors and agents for all removable media.

7 Security

7.1 All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption of the business asset. Due to their small size there is a high risk of the removable media being mislaid lost or damaged, therefore special care is required to physically protect the device and the data. Anyone using removable media to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

7.2 Virus Infections must be prevented from damaging the Councils network and computers. Virus and malware checking software approved by the Council, must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by the virus checking software, before the media is loaded on to the receiving machine.

7.3 Any memory stick used in connection with Council equipment or to store Council material should usually be Council owned. However work related data from external sources can be transferred to the Council network using memory sticks that are from trusted sources and have been checked using current anti-virus software.

7.4 The Council will not provide support or administrator access for any non-council memory stick.

8 Use of removable media

8.1 Care must be taken over what data or information is transferred onto removable media. Only the data that is authorised and necessary to be transferred should be saved on to the device.

8.3 Council material belongs to the Council and any equipment on which it is held should be under the control of the Council and not available to be used for other purposes that may compromise the data.

8.4 All data transferred to removable media should be in accordance with an agreed process established by the Council so that material can be traced.

8.5 The person arranging the transfer of data must be authorised to make use of, or process that particular data.

8.6 Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.

8.7 Encryption must be applied to the data file unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage. If encryption is not available then password control must be applied if removable media must be used for the business purpose.

9 Faulty or Unneeded Storage Devices

9.1 Damaged or faulty media must not be used. The Clerk must be consulted over any damaged equipment, peripherals or media.

9.2 All unneeded or faulty storage devices must be dealt with securely to remove the data before reallocating or disposing of the device.

10 Breach procedures

10.1 Users who do not adhere to this policy will be dealt with through the Councils disciplinary process.

10.2 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

11 Review and Revision

11.1 This policy will be reviewed annually by the Council and revised according to developments in legislation, guidance, accepted good practice and operational use.

12 Employees Guide in Brief

12.1 Data and information are valuable and must be protected.

12.2 Only transfer data onto removable media, if you have the authority to do so.

12.4 All transfer arrangements carry a risk to the data.

12.5 Run the virus checking programme on the removable media each time it is connected to a computer.

12.6 Only use approved products for Council data.

12.7 Activate encryption on removable media wherever it is available and password protection if not available

12.8 Data should be available for automatic back up and not solely saved to removable media.

12.9 Delete files from removable media, or destroy the media, after the material has been used for its purpose.

APPENDIX 9

SOCIAL MEDIA AND ELECTRONIC COMMUNICATION POLICY

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, Facebook page 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.

The Council Facebook page intends to provide information and updates regarding activities and opportunities within our Parish and promote our community positively.

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.
- Refrain from using the Council's Facebook page or Twitter site for commercial purposes or to advertise market or sell products.

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 message/post via Facebook or Twitter 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. Any information posted on the Facebook page not in line with the above criteria will be removed as quickly as practically possible. Repeat offenders will be blocked from the Facebook page. The Council may post a statement that '*A post breaching the Council's Social Media Policy has been removed*'. If the post alleges a breach of a Council's policy or the law the person who posted it will be asked to submit a formal complaint to the Council or report the matter to the Police as soon as possible to allow due process.

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 (clerk@Scaleby.org.uk)

The email account is monitored mainly during office hours, Monday to Friday, and we aim to reply to all questions sent as soon as we can. An 'out of office' message may be used when appropriate.

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.

APPENDIX 10

POLICY AND GUIDELINES FOR BROADCASTING OR USING SOCIAL MEDIA AT COUNCIL MEETINGS

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

SCALEBY PARISH COUNCIL

Policy on the Filming, Photographing, Audio Recording &Social Media Reporting of Public Parish Council and Committee Meetings

In line with the Local Government Audit and Accountability Act 2014.

This Policy identifies the Parish Council's position with the regard to the filming, photographing, audio recording and social media reporting of public Parish Council and Committee meetings. This is in addition to the rights of the press and public to attend such meetings.

Scaleby Parish Council supports the principle of openness and the rights of members of the public and the press to film, photograph, audio record and report on its Council and Committee meetings which are open to the public.

1 RECORDING OF PUBLIC MEETINGS:

1.1 In line with national legislation, the filming, photographing and audio recording of public Parish Council and Committee meetings is permitted.

1.2 Anybody wishing to film, photograph or audio record public meetings is asked to inform the Parish Clerk 24 hours in advance to ensure that the necessary arrangements can be made. This will include arrangements to inform the relevant Parish Council members, guest speakers and public present and, where possible, to provide a separate area for any members of the public who do not wish to be included in the film, photographs or other recordings being made.

1.3 The Council will make the meeting room available to the public for 15 minutes before and after meetings for the setting up and removal of any filming equipment.

1.4 Anybody filming, photographing or audio recording public meetings is required to give due consideration at all times to ensure that there is no disruption to normal proceedings. In this regard, flash photography or additional lighting will not be permitted without the prior permission of the Chairperson.

1.5 In line with national legislation, the reporting, filming, photographing and audio recording must only relate to the public meeting itself and must not extend to anybody seated in the public section who does not form part of the proceedings. Filming, photographing or audio recording a member of the public without their prior express permission is not permitted.

1.6 Anybody wishing to film, photograph or audio record the proceedings must avoid including children or vulnerable adults. Anybody intending to film, photograph or audio record any such individuals seated in the public section is required to first obtain the express permission of their parent or relevant responsible adult to that filming, photographing or audio recording taking place.

2 SOCIAL MEDIA:

2.1 The use of social media for the reporting of the proceedings is permitted during public Parish Council and Committee meetings.

2.2 Anybody wishing to use social media will be required to ensure that this causes no disruption to the running of the meeting. All devices will need to remain on silent for the duration of the meeting.

2.3 Those publishing material from meetings are advised to make themselves aware of the relevant legislation before posting items on social media and web sites.

3 TERMINATION OR SUSPENSION OF FILMING, AUDIO RECORDING & SOCIAL MEDIA REPORTING:

3.1 Where the Chairperson of a relevant meeting considers that any filming, photographing, audio recording or social media reporting activity is causing a disruption to the meeting, the person causing the disruption will be requested to take the appropriate action.

3.2 Should the disruption continue, which makes orderly business impossible, the Chairperson will have the discretion to take whatever action he/she thinks appropriate in accordance with the Parish Council's Standing Orders (eg adjourn the meeting).

3.3 The termination or suspension of filming, photographing, audio recording and social media reporting will occur when:

- there is any public disturbance of the meeting;
- moving around the public section whilst filming;
- the Chair considers that a defamatory statement has been made;
- requests are received from members of the public to cease recording when they speak;
- people are asked to repeat statements for the purposes of recording;
- the meeting formally agrees to exclude the press and public from the meeting due to the exempt nature of the business being discussed; or
- it is considered that continued recording/filming/photographing could infringe the rights of any individual (e.g. an individual in the public section has made a specific request to the Chairperson of the meeting that they do not wish to be filmed, photographed or audio recorded).

4 CONCLUSION:

4.1 The Parish Council welcomes responsible, balanced reporting of its meetings in order to promote greater transparency and awareness of its decision-making.

4.2 The Parish Council requests that anybody recording proceedings provides a balanced representation of the proceedings and does not edit the film or recording in such a way that could lead to misinterpretation of the proceedings or which reflects only a single or particular point expressed at the meeting.

4.3 The formal record of any meeting will be the approved minutes taken by the Clerk to the Parish Council and approved by a vote of its members. These can be found on the Parish Council's website at www.scaleby.org.uk.

APPENDIX 11

PRIVACY NOTICE

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

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
Scaleby 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 Scaleby 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: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY or email clerk@Scaleby.org.uk

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: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY or email clerk@Scaleby.org.uk to request this.

Information Deletion
If you wish Scaleby Parish Council to delete the information about you please contact: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY or email clerk@Scaleby.org.uk 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 Sarah Kyle, Clerk to the Council, to object.

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

Conclusion: In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell or pass your data to third parties. We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We 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).

Complaints
If you have a complaint regarding the way your personal data has been processed you may make a complaint to Scaleby Parish Council's Data Information Officer: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY or email clerk@Scaleby.org.uk and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

APPENDIX 12

EMAIL CONTACT PRIVACY NOTICE

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

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

Scaleby 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 Scaleby 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: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@Scaleby.org.uk

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: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@scaleby.org.uk to request this.

Information Deletion
If you wish Scaleby Parish Council to delete the information about you please contact: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@Scaleby.org.uk 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 Sarah Kyle, Clerk to object.

Rights Related to Automated Decision Making and Profiling
Scaleby 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 Scaleby Parish Council's Data Information Officer: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@scaleby.org.uk and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Summary: In accordance with the law, Scaleby Parish Council only collect a limited amount of information about you that is necessary for correspondence, information and service provision. Scaleby Parish Council) do not use profiling, we do not sell or pass your data to third parties. Scaleby Parish Council do not use your data for purposes other than those specified. Scaleby Parish Council make sure your data is stored securely. Scaleby Parish Council delete all information deemed to be no longer necessary. Scaleby 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).

APPENDIX 13

COUNCILLOR PRIVACY NOTICE

Scaleby
Parish Council

Chairman: Cllr. Linda Thompson

Clerk: Sarah Kyle
Hill House
Walton, Brampton
Cumbria, CA8 2DY
Tel: 01228 231124
email: clerk@scaleby.org.uk
www.scaleby.org.uk

Councillor Privacy Notice
When you sign your acceptance of office and take your seat on Scaleby 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
Scaleby 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 Scaleby 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: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@Scaleby.org.uk

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: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@Scaleby.org.uk to request this.

Information Deletion
If you wish Scaleby Parish Council to delete the information about you please contact: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@Scaleby.org.uk 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 Sarah Kyle, Clerk, to object.

Rights Related to Automated Decision Making and Profiling
Scaleby 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 Scaleby Parish Council's Data Information Officer: Sarah Kyle, Clerk, Scaleby Parish Council, Hill House, Walton, Brampton, CA8 2DY; email: clerk@Scaleby.org.uk and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Summary: In accordance with the law, Scaleby Parish Council only collect a limited amount of information about you that is necessary for correspondence, information and service provision. Scaleby Parish Council do not use profiling, we do not sell or pass your data to third parties. Scaleby Parish Council do not use your data for purposes other than those specified. Scaleby Parish Council make sure your data is stored securely. Scaleby Parish Council delete all information deemed to be no longer necessary. Scaleby 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).

APPENDIX 14

PRIVACY IMPACT ASSESSMENT

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?

APPENDIX 15

SUBJECT ACCESS REQUEST FORM

Scaleby Parish Council

Subject Access Request Form

Process to Action		
Name of requester (Method of communication) Email Address Phone number Postal Address		
Date Subject Access Request made		
Is the request made under the Data Protection Legislation	Yes	No
Date Subject Access Request action to be completed by (One month after receipt time limit)		
Extension to the date of reply requested (An extension of another two months is permissible provided it is communicated to the subject within the one month period)	Yes	No
Extension date advised to the Subject Requester and method of contact		
Identification must be proven from the below list: Current UK/EEA Passport UK Photo card Driving Licence (Full or Provisional) EEA National Identity Card Full UK Paper Driving Licence State Benefits Entitlement Document State Pension Entitlement Document HMRC Tax Credit Document Local Authority Benefit Document State/Local Authority Educational Grant Document HMRC Tax Notification Document Disabled Driver's Pass Financial Statement issued by bank, building society or credit card company Utility bill for supply of gas, electric, water or telephone landline A recent Mortgage Statement A recent council Tax Bill/Demand or Statement Tenancy Agreement Building Society Passbook which shows a transaction in the last 3 months and their address		
Verification sought that the Subject Access request is substantiated	Yes	No
Verification received	Yes	No
Verification if the Council cannot provide the information requested	Yes	No
Is the request excessive or unfounded?	Yes	No
Request to be actioned	Yes	No
Fee to be charged (Subject Access requests must be undertaken free of charge to a requester	Yes	No

unless the legislation permits a reasonable charge)		
If the request is to be refused, action to be taken and by whom.		
Changes requested to data/ or removal		
Complaint Process (Where a requestor is not satisfied with a response to a SAR, the council must manage this as a complaint)		
Completion date of request		
Date complaint received by requested and details of the complaint		
Date complaint completed and outcome		

Categories of Data to Check

Data	Filing Cabinet	Laptop	Checked	Corrected/Deleted	Actioned by
HR					
Democracy					
Statutory Function					
legal					
Business					
Legal requirement					
General Data					
Consultation Data					

APPENDIX 16

DATA BREACH REPORTING FORM

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	