

Redgrave Parish Council

Information Protection Policy

1 Purpose

- 1.1 Information is a major asset that Redgrave Parish Council has a duty and responsibility to protect.
- 1.2 The purpose and objective of this Information Protection Policy is to specify the means of information handling and transfer within the Council.

2 Scope

- 2.1 The Information Protection Policy applies to all Councillors, Committees, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Council purposes.
- 2.2 Information takes many forms and includes:
 - hard copy data printed or written on paper
 - data stored electronically
 - communications sent by post / courier or using electronic means
 - stored tape or video
 - speech

3 Information Storage

- 3.1 All electronic information will be stored on centralised facilities to allow regular backups to take place.
- 3.2 Information will not be held that breaches the Data Protection Act (1998) or formal notification and guidance issued by Redgrave Parish Council. All personal identifiable information will be used in accordance with the Caldicott Principles (Every single proposed use or transfer of identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.)
- 3.3 A records management and retention policy will be followed (Appendix A).
- 3.4 Staff should not be allowed to access information until the Council is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- 3.5 Databases holding personal information will have a defined security and system management policy for the records and documentation.
- 3.6 This documentation will include a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection Notification.
- 3.7 Files which are listed by Redgrave Parish Council as a potential security risk should not be stored on the network, except for in designated application storage areas.

Redgrave Parish Council Information Protection Policy

4 Disclosure of Information - Computer and Paper Based

- 4.1 The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is to be reported to the Data Control Officer (Clerk) who will take appropriate action.
- 4.2 Do not remove printed information from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances
- 4.3 Protectively marked, personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.
- 4.4 Disposal methods for waste computer printed output and other media must be in accordance with the Council's disposal policy.
- 4.5 Distribution of information should be via the most secure method available.

5 Disclosure of Information – Telephone and E-mail

- 5.1 Where this involves the exchange of sensitive information then the following procedures will be applied.

6 Telephone calls:

- 6.1 Verify the identification of members before disclosing information. If in doubt, return their call using a known telephone number.
- 6.2 For external callers, verify their identity and their need to know the requested information. Telephone them back before releasing information and ask the caller to provide evidence of their identity (this could be passport, driving license, household bill).
- 6.3 Ensure that you are authorised to disclose the information requested.
- 6.4 Ensure that the person is entitled to be given this information.
- 6.5 Ensure that the information you give is accurate and factual.

7 Disclosure of information by email:

- 7.1 Personal or sensitive information is at risk if sent outside of the Council's network of members and employees.
- 7.2 Email should not be used for sending personal or sensitive information unless technical measures, such as encryption, are in place to keep the message secure.
- 7.3 The sender should be satisfied of the identity of the recipient. If in doubt the email should not be sent, and alternative methods should be used.

Redgrave Parish Council Information Protection Policy

- 7.4 No identifiable personal information should be included when sending on emails to individuals or organisations outside of the Council's network, including email addresses, without the permission of the original email owner.
- 7.5 The recipient should be aware that Council emails are prohibited from being forwarded, copied or blind copied to any third party within or outside of the Council.
- 7.6 Any Councillor email contact with a member of the public shall be directed to the Council's Office for the attention of Data Control Officer (Clerk).

8 Sharing of Personal Information

- 8.1 Information relating to individuals shall not be shared with other authorities without the agreement of the Data Control Officer (Clerk).
- 8.2 Staff should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

Redgrave Parish Council

Information Protection Policy

APPENDIX A

Retention of Documents and Records

This policy details the minimum retention time required for council documents before disposal in order for the council to comply with the Freedom of Information Act 2000 Publication Scheme. Where variable times are indicated the Council will review storage after the minimum period has elapsed.

Document	Minimum Period	Reason
MINUTES		
Approved minutes	Indefinite	Archive
Draft/rough/notes of minutes taken at meetings	Until minutes are approved	Management
FINANCE		
Receipt and Payment Accounts	Indefinite	Archive
Paid invoices	6 years	VAT
VAT records	6 years	VAT
Bank Statements	Last completed audit year	Audit
Paying in books	Last completed audit year	Audit
Cheque stubs	Last completed audit year	Audit
Scales of fees and charges	5 years	Management
Members allowances register	6 years	Tax, Statute of Limitations
PLANNING		
Applications	Retain as long as useful	Held at District Council
Permissions	Retain as long as useful	Held at District Council
Refusals	Retain as long as useful	Held at District Council
INSURANCE		
Insurance policies	2 years	Management
Certificates of Employers' Liability Insurance	40 years	Limitation period
OTHER		
Quotations and tenders	12 years / Indefinite	Statute of Limitations
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
Routine correspondence, papers & emails	Retain as long as useful	Management