Treverbyn Parish Council

General Data Protection Regulation (GDPR) Policy

1. Introduction

Treverbyn Parish Council ("the Council") is committed to protecting the privacy and rights of individuals in accordance with the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations (where applicable)

The Council recognises its responsibilities as a Data Controller and is committed to processing personal data lawfully, fairly, transparently and securely.

This policy sets out how the Council manages personal data and the responsibilities of councillors, employees, volunteers and co-opted members.

2. Scope

This policy applies to all personal data processed by the Council, including data relating to:

- Residents
- Employees
- Councillors
- Contractors
- Suppliers
- Service users
- Volunteers
- Members of the public
- Correspondents and complainants

The policy applies to:

- Electronic records
- Emails
- Paper records
- Audio or visual recordings
- Online systems and cloud services

3. Definitions

Personal Data

Any information relating to an identified or identifiable living individual.

Examples include:

- Names
- Addresses
- Telephone numbers
- Email addresses
- Photographs
- Financial details
- IP addresses

Special Category Data

Personal data requiring additional protection, including information about:

- Health
- Ethnicity
- Religious beliefs
- Political opinions
- Trade union membership
- Sexual orientation

Processing

Any activity involving personal data, including:

- Collection
- Storage
- Use
- Sharing
- Disclosure
- Deletion

4. Data Protection Principles

The Council shall ensure that personal data is:

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Retained only as long as necessary
6. Processed securely
7. Managed in a way that demonstrates accountability

5. Lawful Basis for Processing

The Council shall only process personal data where a lawful basis exists under UK GDPR.

These may include:

- Legal obligation
- Public task
- Consent
- Contract
- Vital interests
- Legitimate interests (where applicable)

The Council shall identify the lawful basis before processing personal data.

6. Responsibilities

6.1 The Council

Treverbyn Parish Council is the Data Controller and is responsible for ensuring compliance with data protection legislation.

The Council shall:

- Adopt appropriate policies and procedures
- Ensure personal data is processed securely
- Maintain appropriate records
- Respond to data protection requests
- Provide appropriate training and guidance

6.2 The Clerk

The Clerk shall oversee day to day data protection compliance and act as the primary point of contact for data protection matters.

Responsibilities include:

- Managing information requests
- Reporting data breaches
- Maintaining records
- Advising councillors and staff
- Ensuring policies are reviewed

6.3 Councillors, Staff and Volunteers

All persons handling Council information must:

- Follow this policy
- Protect personal data
- Only access information necessary for their role
- Keep information secure
- Report concerns or breaches immediately

Personal data obtained through Council activities must not be used for personal, political, or unauthorised purposes.

7. Information Security

The Council shall take reasonable and proportionate measures to protect personal data.

Measures may include:

- Password-protected devices
- Secure Council '.gov.uk' email accounts
- Anti-virus and cyber security protections
- Access controls
- Secure storage
- Data backups
- Staff awareness and training

7.1 Personal Devices (BYOD)

Some councillors use personal devices for Council business and meetings.

Where personal devices are used:

- Devices must be password or biometric protected
- Software should be kept updated
- Council information must be stored securely
- Personal data must not be shared inappropriately
- Data should be deleted when no longer required

Councillors must take reasonable steps to protect personal data accessed through personal devices.

8. Email and Communications

Council business should be conducted through official Council communication systems wherever practicable.

Treverbyn Parish Council uses official '.gov.uk' email accounts for Council business.

Users must:

- Use Council email responsibly
- Avoid sending unnecessary personal data
- Use care when sending confidential information
- Be aware that emails may be subject to disclosure under legislation

9. Data Sharing

The Council may share personal data where:

- Required by law
- Necessary for official Council functions
- Consent has been obtained
- Appropriate safeguards are in place

Personal data shall not be shared unnecessarily.

Where third-party services process data on behalf of the Council, appropriate contractual arrangements shall be in place where required.

10. Data Retention

The Council shall retain records only for as long as necessary and in accordance with its Retention Policy.

When no longer required, personal data shall be securely:

- Deleted
- Destroyed
- Shredded
- Permanently removed from electronic systems where appropriate

11. Individual Rights

Individuals have rights under UK GDPR, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (where applicable)
- The right to restrict processing
- The right to object
- The right to data portability (where applicable)

Requests should normally be made in writing to the Clerk.

The Council shall respond within statutory timescales.

12. Subject Access Requests

Individuals may request access to personal data held about them.

The Council shall:

- Verify identity where necessary
- Respond within one calendar month unless exemptions apply
- Provide information in accordance with legal requirements

The Council may refuse requests where exemptions apply under legislation.

13. Data Breaches

A personal data breach includes:

- Loss of personal data
- Unauthorised access
- Accidental disclosure
- Cyber incidents affecting personal data

All breaches or suspected breaches must be reported immediately to the Clerk.

The Council shall assess breaches and report them to the Information Commissioner's Office (ICO) where legally required.

14. Freedom of Information and Transparency

The Council shall balance transparency obligations with data protection requirements.

Personal information shall be redacted where appropriate before publication or disclosure.

Councillors and staff must take care when publishing:

- Agendas
- Minutes
- Reports
- Correspondence
- Online content

15. Training and Awareness

Appropriate data protection awareness and guidance shall be provided to councillors and staff.

Individuals handling personal data are expected to maintain awareness of good information governance practices.

16. Monitoring and Compliance

The Council reserves the right to monitor compliance with this policy and related procedures where lawful and proportionate.

Failure to comply with this policy may result in:

- Withdrawal of access to information systems
- Internal disciplinary procedures
- Referral to relevant authorities where appropriate

17. Review

This policy shall be reviewed annually or sooner if required due to legislative, operational, or technological changes.

18. Adoption

Adopted by Treverbyn Parish Council on: