

FINDOCHTY COMMUNITY COUNCIL

Data Protection Policy

Authority	UK General Data Protection Regulation (UK GDPR) / Data Protection Act 2018
ICO Registration	Registered as required by Moray Council
Version	1.0
Date Adopted	[date]
Review Period	Annual

This policy sets out how Findochty Community Council collects, uses, stores and protects personal data. It applies to all members, volunteers and anyone acting on behalf of the Community Council.

1. Introduction

Findochty Community Council (FCC) handles a small amount of personal data in the course of its work - primarily contact details of members, residents who get in touch, and those who attend or participate in community events and surveys.

As an organisation that processes personal data, FCC is registered with the Information Commissioner's Office (ICO), as required by Moray Council. We are committed to handling all personal data responsibly, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Secretary is the lead officer responsible for data protection within FCC. Day to day responsibility for financial records rests with the Treasurer.

2. The Seven Data Protection Principles

UK GDPR requires that all personal data is handled in accordance with seven principles. FCC is committed to meeting each of them:

Principle	What it means in practice for FCC
Lawful, fair and transparent	We only collect data we have a legitimate reason to hold, and we are open with people about how we use it.
Purpose limitation	Data is collected for a specific purpose and not used for anything else without good reason.
Data minimisation	We only collect what we actually need. We do not gather information that serves no clear purpose.
Accuracy	We take reasonable steps to keep personal data accurate and up to date, and correct it when we become aware it is wrong.

Storage limitation	We do not keep personal data for longer than necessary. Retention periods are set out in our Records Retention Policy.
Integrity and security	We store data securely and protect it from loss, unauthorised access or misuse.
Accountability	We can demonstrate that we comply with these principles. This policy, our Data Register and our ICO registration are part of that evidence.

3. What Personal Data We Hold

FCC holds a limited amount of personal data. This typically includes:

- Names, addresses, telephone numbers and email addresses of Community Council members
- Contact details of residents who write to or email the council
- Names and contact details of individuals involved in specific projects or events
- Survey responses where individuals have chosen to identify themselves
- Photographs taken at community events, where used for publicity purposes

We do not collect sensitive personal data (such as health information, financial details or political opinions) unless there is a specific and necessary reason to do so.

4. Lawful Basis for Processing

Under UK GDPR, every instance of processing personal data must have a lawful basis. FCC relies on the following:

Legitimate interests

Most of the personal data FCC handles is processed on the basis of legitimate interests - for example, holding members' contact details to conduct council business, or corresponding with residents about local matters. This is the most appropriate basis for the routine administrative work of a community council.

Legal obligation

Some processing is required by law or by the Moray Community Council Scheme of Establishment - for example, maintaining membership records and submitting information to Moray Council.

Consent

Where neither of the above applies, we will ask for explicit consent before collecting or using personal data. This is most likely to apply to:

- photographs used for publicity or online publication
- survey responses collected for specific purposes
- mailing lists or newsletters

Consent must be freely given, specific and unambiguous. Where we rely on consent, individuals have the right to withdraw it at any time. Consent for one purpose does not automatically apply to another.

Where photographs are taken at community events for publicity use, we will make this clear at the time. Individuals who do not wish to be photographed should let the photographer know.

5. How We Use Personal Data

FCC uses personal data only for the purposes for which it was collected. This includes:

- Conducting Community Council business and communicating with members
- Responding to enquiries and correspondence from residents
- Organising community events and activities
- Carrying out community surveys and consultations
- Fulfilling our statutory obligations under the Moray Community Council Scheme
- Publishing meeting agendas, minutes and public notices

Minutes of meetings are public documents and will name members present and record contributions made. This is a standard and necessary part of Community Council governance and does not require individual consent.

6. Sharing Personal Data

FCC does not sell or share personal data with third parties for commercial purposes.

We may share personal data in the following limited circumstances:

- With Moray Council, where required by the Scheme or for the administration of Community Council business
- With Police Scotland or other public bodies, where necessary to deal with a specific matter
- With other organisations directly involved in a community project, where individuals have been made aware

Any organisation with whom we share personal data is expected to handle it in accordance with UK GDPR.

Where FCC uses external online services (such as survey tools, email platforms or cloud storage), we will use reputable providers who comply with UK data protection law. We will not use services that transfer data outside the UK unless appropriate safeguards are in place under the UK's international transfer framework.

7. Security

FCC will take reasonable and proportionate steps to keep personal data secure. This includes:

- Storing digital records on password-protected devices or secure cloud services
- Using strong passwords and, where available, two-factor authentication
- Keeping paper records containing personal data in a secure location
- Ensuring that only members who need access to personal data can access it
- Securely deleting or destroying personal data when it is no longer required, in line with the Records Retention Policy

8. Data Register

FCC maintains a Data Register recording:

- what categories of personal data are held
- the lawful basis on which each category is processed
- how long each category is retained
- where the data is stored and who has access

The Data Register is maintained by the Secretary and reviewed annually. It is available for inspection by members of the Community Council.

9. Individual Rights

Under UK GDPR, individuals have the following rights in relation to their personal data:

- Right of access - to request a copy of the personal data FCC holds about them
- Right to rectification - to ask us to correct inaccurate or incomplete data
- Right to erasure - to ask us to delete their data, where there is no lawful reason to retain it
- Right to restrict processing - to ask us to limit how we use their data in certain circumstances
- Right to object - to object to processing based on legitimate interests
- Right to withdraw consent - where processing is based on consent, to withdraw it at any time

Requests should be made in writing to the Secretary. FCC will respond within one month, in accordance with ICO guidance. Where a request is complex or there are multiple requests, this period may be extended by a further two months, with notice given to the individual.

10. Data Breaches

A data breach occurs when personal data is accidentally or unlawfully lost, destroyed, altered, disclosed or accessed without authorisation.

If a breach occurs or is suspected, the Secretary (or the member who becomes aware of it) must:

- Immediately inform the Chairperson and at least two other members of the council
- Assess the nature and likely impact of the breach on affected individuals
- Report the breach to the ICO within 72 hours if it is likely to result in a risk to individuals' rights and freedoms
- Notify affected individuals directly if the breach is likely to result in a high risk to their rights and freedoms
- Report the breach and any remedial action taken to the next Community Council meeting

Not all breaches need to be reported to the ICO - only those that are likely to result in a risk to individuals. However, all breaches must be recorded internally, regardless of whether they are reported.

11. Complaints

Any complaint about how FCC has handled personal data should be made in writing to the Secretary and will be handled under the Community Council's Complaints Procedure.

If a complainant remains dissatisfied after FCC has responded, they have the right to complain directly to the Information Commissioner's Office:

- Website: ico.org.uk
- Telephone: 0303 123 1113

12. Review

This policy shall be reviewed annually and updated as required. Any material changes will be approved by the Community Council at a meeting.

Adopted by Findochty Community Council on: _____

Signed (Chairperson): _____

Signed (Secretary): _____