1.11
Data Protection and Privacy Policy

Introduction

Moray Community Councils has a responsibility under the Data Protection Act 2018 to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. This Policy is a statement of what Community Councils does to ensure its compliance with the Act.

Moray Community Councils is committed to protecting the rights and privacy of its members, community members and other individuals in accordance with the Regulations. This Data Protection Policy applies to all members of the Community Council, volunteers and contractors working with the Community Council. The Policy provides a framework within which Moray Community Councils will ensure compliance with the requirements of the Act and will underpin any operational procedures and activities connected with the implementation of the Act.

As a matter of good practise, any other organisations working with the Community Council, such as the Local Authority or Police Scotland and who may need access to personal information such as contact details in order to deal with a complaint or local issue, will be expected to have read and to comply with this policy.

Background

The Data Protection Act 2018 governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals about whom data is held (the "data subjects") can have a certain amount of control over the way in which it is handled.

All data covered by the Act must be handled in accordance with the Six Data Protection Principles.

I. **Lawful, fair and transparent**: There has to be legitimate grounds for collecting the data and it must not have a negative effect on the data subject or be used in a way they wouldn't expect.
II. **Limited for its purpose**: Data should be collected for specified and explicit purposes and not used in a way someone wouldn't expect.
III. **Adequate and necessary**: It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected. CRC will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.
IV. **Accurate and Up to Date:** Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate.

V. **Not kept longer than needed**: Data should not be kept for longer than is needed, and it must be properly destroyed or deleted when it is no longer used or goes out of date.

VI. **Integrity and Security**: Data should be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, loss, damage or destruction, and kept safe and secure.

Policy Statement

The Community Council is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under the Data Protection Act 2018 and professional guidelines. The Community Council will use all appropriate and necessary means at its disposal to comply with the Data Protection Act and associated guidance.

Responsibilities

- Community Councils are not required to have a 'Data Controller' but it is the responsibility of the organisation to determines the purpose for which and the manner in which any personal data are, or are to be processed.
- The Community Council secretary will be responsible for ensuring member's awareness, policy compliance and general security of personal information.
- This policy applies to all personal information held by the Community Council Personal data collected by the Community Council may include:
    - Individuals names
    - Addresses
    - Telephone numbers
    - Email addresses
- To ensure we are complying with our legal requirements,
- This policy will be periodically reviewed.
- The Community Council will register with the Information Commissioner's Office (ICO) as an organisation which processes personal information.

Lawful, fair and transparent processing

As a Community Council we process personal information to enable us to serve and represent the interests of the community within the local area.

To ensure its processing of data is lawful and transparent, the Community Council will maintain a Data Register recording:

- what data is being kept;
- under what lawful processing data (see 5) is being used;
- Details of the level of risk involved with any data breach.
- The Data Register will be reviewed annually

- Individuals have various rights over their personal information within the Regulation. Any request by individuals to access, alter or delete their personal information will be dealt within the Guidelines set out by the ICO.

Lawful Purpose

As a Community Council, we will process personal information to enable us to serve and represent the interests of the community within the local area. The information we process may include personal contact details and family, lifestyle and social circumstances in relation to the above purpose.

The purpose of processing will be noted in the Data Register.

Where consent is needed, evidence of opt-in consent shall be kept with the personal data.

Where any communication is sent to individuals either digitally or printed material, it will include a clear statement on data protection and how to evoke their consent. Systems will be in place to ensure that if such a request is received it is dealt with in a timely and accurate manner.

Consent

We will obtain consent for all personal information through;

- Verbal communication where verbal consent will be sought. Where possible this will be followed up with an email or other means of consent.
- Email communication wherein consent will be sought on the first email and kept with the personal information.
- Events or surveys where consent will be stated as a privacy notice on the written material and a signature or opt-in tick box will indicate consent.
- Consent will be obtained for one purpose and not automatically applied to other uses.
- If the individual is under 16 years of age, we will ask for parental/guardian consent.
- All media including photographs, videos will be obtained in writing if the material is being used for any publicity purposes, is to be used online or if it will be shared with others.

Data Minimisation

The Community Council shall ensure that all personal data collected is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- The Community Council shall take all reasonable steps to ensure all stored personal data is accurate.

- The Community Council shall take all reasonable steps to ensure all stored personal data is kept up-to-date through an annual review and systems to ensure inaccurate data is rectified within the Guidelines set out by the ICO.
- All changes to data, whether by individual request or other means, will be recorded in the Data Register.

Archiving/deletion

To ensure that personal data is kept for no longer than necessary, the Community Council shall record archiving and retention rules for each area in which personal data is processed and review this process annually.

The archiving and retention rules shall consider what data should/must be retained, for how long, and why.

On deleting personal information, the Community Council will ensure all Data is securely destroyed and cannot be retrieved. All deletion will be recorded in the data Register.

Security and Confidentiality

The Community Council will ensure that all personal data is stored securely including data stored in paper based files which should be in locked cabinets and digital files which should be held on secure computers.

Access to personal data will be restricted to those who need the information to lawfully process it as previously mentioned.

All computers or digital systems used to store or process data should be protected by a strong password or log in which is changed frequently and up-to-date security software including anti-virus and firewalls. Data should not be shared through insecure email systems or kept on a USB storage device unless similar security as mentioned in in place.

When using external companies or online providers, the Community Council will ensure they either operate within the European Union's GDPR or is a member of Privacy Shield (companies out with the EU who comply with GDPR principles - https://www.privacyshield.gov/)

When personal data is deleted this should be done safely such that the data is irrecoverable.

Appropriate back-up and disaster recovery solutions shall be in place.

Breach

If a security breach whether accidental or unlawful breach occurs leading to destruction, loss, alteration or unauthorised disclosure of personal data, the Community Council will bring together three or more members of the Community Council including the person responsible for data protection, to assess the breach. This group will promptly assess the risk to people's rights and freedoms and if it is appropriate report this breach to the ICO.

This group will assess if the breach has a high risk of adversely affecting an individual's rights and freedoms, and if so contact the individual without delay.

This group will report back to the next Community Council meeting and recommend any alterations or strengthening of the Community Council's data protection policy or procedures.

Rights of Individuals

The Community Council will adhere to the individual's rights under GDPR. These are;

- make it easier for people to **withdraw their consent** for their personal data to be used
- enshrine the "**right to be forgotten**" into UK national law, allowing people to ask for their data to be deleted e.g. by social media companies and online traders
- require companies to obtain **explicit consent** when they process sensitive personal data
- expand the **definition of personal data** to include IP addresses, biometric data and cookies
- allow people to **obtain the information** organisations hold on them much more freely, via subject access requests
- Provide data subjects with **broader rights** to claim compensation for breaches where "other adverse effects" are suffered. Currently,
- Compensation can only be claimed for breaches that cause financial loss or distress.

Complaints

Any expression of dissatisfaction from an individual with reference to the Community Councils handling of personal information will be treated as a complaint under the Community Council's complaint's process. The Secretary will respond to the complaint.

Should the complainant remain dissatisfied with the outcome of their complaint the Community Council, a complaint can be made to the Information Commissioner's Office who will investigate the complaint and take action where necessary.