Midlothian Community Councils
Managing your information.
Information and Data Protection

Purpose

Community Councils will create and receive information. It is important that these records and data are managed in a robust, consistent, and lawful way.

This guidance is designed to help Community Councils manage the information they deal with appropriately. It sets out how records should be stored, retained, accessed, and transferred, as well as how personal data should be handled. This will help Community Councils meet their obligations under the EU General Data Protection Regulation (GDPR) and Data Protection Act 2018.

Managing Records

Community Councils will create, receive, use, and manage a variety of information in the course of business. These will include core records, such as minutes of meetings and supporting records, but other records such as correspondence, planning information, reports, financial transactions, and survey data. Administration information will also be generated and need to be managed.

It is a requirement within the Midlothian Scheme for the Establishment of Community Councils that each Community Council makes available to the Council the records which the council requires. The Scheme sets out minimum content for key records such as Minutes of Community Council meetings.

Accordingly, each Community Council must:

- When creating and maintaining records that meet the requirements of both the Midlothian Scheme for the Establishment of Community Councils and the Scottish Government's Good Practice Guidance (see page 40).
- Ensure that draft copies of Minutes are forwarded to Midlothian Council at this email address - midlothianccminutes@midlothian.gov.uk.
- Ensure that their Secretary and Treasurer are aware of their responsibilities around managing the records of the Community Council and that they have adequate support to do so.
- Document what records will be created or held by the Community Council, how they will be stored (e.g., on computer, encrypted removable media, by email etc.) and in whose custody, they will be in. This document should be reviewed and approved by the Community Council at least annually. A suggested template is provided in Appendix 1.

- Ensure that all Community Council records are retained for at least the retention periods required by Midlothian Council as set out in Appendix 2.
- Ensure that all Community Council records containing sensitive or personal data are securely destroyed when they are no longer needed.
- Documenting the date and authorisation of the destruction of Community Council records.

When an individual ceases to be a Community Council office Bearer, they must ensure that all records they hold relating to the Community Council are appropriately reviewed and transferred to the Secretary or Treasurer. Community Council Office Bearers should not retain any information relating to their work with the Community Council when they are no longer a part of it.

Protecting records

Protect personal data is most important. Community Council Office Bearers should ensure that any records within their possession are protected to prevent unauthorised or inappropriate access and use. If records are retained within the home, held either electronically or in paper, suitable controls should be in place to protect those records, and the information they contain, from accidental access. Various measures can be used, such as:

- Password protecting all folders when storing information on home computers.
- Avoid using personal email address and create a generic email address for Community Council business. Ensure passwords are not shared.
- Use locked storage to store any Community Council records, particularly those which contain sensitive or personal data.

If a Community Council Office Bearer and/or member suspects that information within their possession may have been accessed inappropriately, they should report their concern to the Community Council Secretary or Chairperson to ensure that appropriate action can be taken.

Managing Personal Data

Community Councils will process personal data. Personal data is any information relating to an identified or identifiable natural person. It is basically any information that relates to a living individual, such as their name, address, and bank details.

'Processing' is an all-encompassing term: it means collecting, storing, sharing, managing, and disposing of personal data (basically doing anything with it).

The EU General Data Protection Regulation and the Data Protection Act 2018 together provide a framework which governs how organisations should manage personal data lawfully. It is enforced and regulated by the UK Information Commissioner (ICO).

Organisations must manage personal data in accordance with the six data protection principles, detailed below:

- Information must be processed lawfully, fairly and in a transparent manner.
- Information must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Information must be adequate, relevant, and limited to what is necessary.
- Information must be accurate and, where necessary, kept up to date.
- Information must be kept in a form which permits identification of data subjects for no longer than is necessary.
- Information must be processed in a manner that ensures the appropriate security of the personal data.

The following sections provide a summary of the key features of the legislation and issues which Community Councils will need to consider ensuring compliance with the principles set out above. A check list of recommended actions is set out in appendix 4.

Responsibility for data protection

To comply with these principles, it is advised that Community Councils nominate someone as the person responsible for data protection matters.

Registering with the Information Commissioners Office (ICO)

Organisations which process personal data, such as Community Councils, are known as Data Controllers. While the amount of personal data Community Councils process may be small, you are strongly advised to register with the ICO. Registration currently costs £40. Further information on the registration process can be found on the ICO website.

Processing personal data lawfully

Organisations can only process personal data when they meet a lawful condition under data protection law. The processing condition relevant to Community Councils is most likely to be 'consent'. In other words, you must ask for and get an individual's consent before you can use their personal data. For example, when collecting contact details for each Community Council member, get them to sign a mandate giving you permission to use their personal data. You would only have to do this once when they join the Community Council.

It is also helpful to retain mandate forms so you can demonstrate compliance with data protection law. This will help you to meet the accountability principles enshrined within the legislation.

Note: Individuals can withdraw consent at any time. If that happens, you must cease using their data.

Community Councils may also receive information about third parties, for example in connection with being consulted over planning or licensing applications. The lawful basis for processing this sort of personal information is likely to be that it is necessary for you to use this personal information to perform a task conducted in the public interest by the Community Council. Consent would not be necessary (or appropriate) in these circumstances.

The lawful basis for processing personal data must be set out in a document known as a 'Record of Processing'. Further information is available on the ICO website. However, given the limited processing Community Councils are involved in, this information could be included within your privacy notice (see below).

Telling people what you do with their personal data.

It is important that individuals understand why and how their personal data is collected. This information must be set out in a privacy notice. Privacy notices can be made available on a website, through a leaflet or on any documentation that collects personal data. Privacy notices are important: transparency around what we do with peoples' data is a fundamental aspect of data protection law.

The ICO has produced detailed guidance on privacy notices, including templates. The Council's website (Midlothian Council Privacy information) has numerous examples covering the many different functions the council carries out.

There is also a template (created by Rosewell CC) on the Midlothian Federation of Community Councils website in the 'policies' section.

Collecting personal data

Community Councils should collect personal data *only* when it is necessary and appropriate (e.g., a CC Secretary will need to collect contact information for Office Bearers and Members). Also, you should only collect what personal data you need to allow you to process it: do not collect excessive amounts of personal data if it is not required. For example, if someone wants to be contacted by email only, do not collect additional contact details, unless you have their permission.

Sharing personal data

Only share personal data that is needed to deal with a particular situation. For example, if a Community Council need to share personal data with another organisation to help facilitate a participation request under the Community Empowerment (Scotland) Act 2015, only share what you have to, and make sure that the individual to whom the data relates is happy for you to do so.

If Community Councils need to share personal data with any other organisation on a regular basis, this may require arrangements to be formalised through an information sharing agreement. An exception to this would be if, for example, the police required personal data to be shared in order to investigate a crime. Whatever the circumstances, it is always best practice to keep a record of what information is shared, with whom and why.

Using personal data

The personal data you collect can only be used for a specific purpose (e.g., to keep Community Council members updated about community activities and events). However, just because you hold that information does not mean that you can use it for a different purpose. For example, you could not use resident contact details to circulate a newsletter if those details were provided to inform an on-line survey. If you wanted to do that you would need to ask people at the time you were collecting their data and seek their permission to do so.

Accuracy of personal data

Data protection law places a responsibility on data controllers to keep personal data up to date (e.g., contacts lists). You should carry out periodic checks to make sure the personal data you hold is accurate.

Keeping personal data

Personal data should not be kept for any longer than is necessary. The retention advice set out in appendix 2 will help you with this.

Protecting personal data

The need to protect personal data is a key principle within data protection law. The previous section on 'protecting information' provides helpful advice. In addition, if Community Councils use their website to process personal data (e.g., to conduct a local survey), they must ensure that appropriate security controls are in place to protect it.

Breaches

It is important to prevent personal data from being lost, damaged, or disclosed without authorisation. However, incidents do occur which are known and classified as data protection breaches. These can include:

- Personal information uploaded to the website in error.
- Records damaged or destroyed by fire, flood, or other means.
- The theft or loss of hardware (e.g., laptops, portable devices).
- Disclosure of personal information in error (e.g., a letter or email sent to the wrong constituent, or sending a newsletter to a distribution group using the *To*: field instead of *BCC*:).
- The theft or loss of records containing personal information (e.g., portable devices, paper files).

If a breach does occur then unless there is a minimal risk to the rights and freedoms of those affected, it is necessary to notify the ICO. The quicker breaches are reported and contained the better. Any reportable breach must be reported to the ICO within 72 hours of the data controller learning about it.

This period of 72 hours does not stop for weekends or bank holidays so if something does go wrong it is essential that whoever is responsible for data protection in your Community Council is informed promptly and that that person then notifies the ICO. Data breaches can lead to fines and other sanctions from the ICO. Failure to notify a breach can also lead to sanctions. The Council should be informed promptly if you suffer a data breach which needs to be notified to the ICO.

Individual Rights

Individuals have certain rights under data protection law, these include the right to ask what information is held about them, to ask for their personal data to be rectified if it is inaccurate, or not to be processed further. Individuals also have a right to prevent their information from being used for direct marketing. If you receive such requests, in most cases you will need to comply with them in full within one month of receiving the request.

Further Information

The ICO website contains a lot of useful guidance and also has a help line for small organisations which Community Councils may want to make use of – this is 0303 123 1113.

ICO in Scotland Contact Details

The Information Commissioner's Office – Scotland
Queen Elizabeth House
Sibbald Walk
Edinburgh
EH8 8FT

Telephone: 0303 123 1115
Email: scotland@ico.org.uk

Appendix 1: Template for recording general principles of record keeping.

Record keeping responsibilities		Contact Details
Chair		
Secretary		
Treasurer		

Other Community Councillors responsible for records		
Name	Responsibilities	Contact Details

Records Overview			
Activity	Format *(e.g., emails, PDFs, paper etc. – you should cover all formats in use)*	Storage Location / Custody	Notes
Minutes, agenda & meeting papers			Main council, sub-groups, and joint meetings with other bodies
Accounts			Annual Statement of Accounts
Payments			Cheques, invoices & expenses
Bank account management			
Newsletters			
Surveys by council			
Consultation responses by council			
Membership / contact lists			
Official correspondence			
Event planning			

Records Overview Cont'd			
Activity	Format *(e.g., emails, PDFs, paper etc. – you should cover all formats in use)*	Storage Location / Custody	Notes

Appendix 2: Minimum Record Retention Periods for Community Council Records

Record Types	Retention Requirements
Core meeting records (to include approved minutes, agenda, and supporting reports)	Retain Permanently *Community Councils will routinely transfer minutes of their meetings to Midlothian Council.*
Consultations; responses to planning and licensing applications	Date of last action + 5 years, then DESTROY
Media relations; correspondence, articles, monitoring	Date of last action + 5 years, then DESTROY
Other correspondence; including with individuals and other organisations	Date of last action + 5 years, then DESTROY
Newsletters	End of Calendar Year + 3 years, then DESTROY
Projects (including campaigns)	Project closure + 2 years (small scale) or 10 years (large scale), then REVIEW
Surveys; admin, preparation & responses	Date of last action + 3 years, then DESTROY
Surveys; final report & analysis	Publication + 5 years, then REVIEW
Accounting records	End of Financial Year + 6 Years, then DESTROY
Raising, receiving & spending of domestic funding	End of Financial Year + 6 Years, then DESTROY
Raising, receiving & allocation of EU sourced funding	*For advice on EU funding record retention requirements contact the council department you are involved in the EU funded project with.*
Routine administration of bank accounts	Closure of account + 6 years, then DESTROY
Deposits/withdrawals/transfer of funds	End of Financial Year + 6 Years, then DESTROY

Appendix 3: Template Disposal Register

Disposal Reference	Description of disposal	Retention Period	Officer Authorisation	Authorised Date	Disposal Date	Format	Notes

Appendix 4: Compliance Checklist

Ref	Action	Tick
1.	Assign responsibility for data protection.	
2.	Register Community Council with ICO	
3.	Develop a privacy notice and tell people what you do with their data.	
4.	Only collect what personal data you need.	
5.	Understand how personal data can be used.	
6.	Keep any personal data you may hold up to date.	
7.	Ensure that personal data is properly protected.	
8.	Develop retention rules & do not keep data for longer than is necessary.	
9.	Understand what to do if a breach occurs.	
10.	Document your data protection procedures	