

Managing your records and protecting your data

Purpose

This guidance is designed to help Community Councils appropriately manage information in a robust, consistent and lawful way. It sets out how records should be stored, retained, accessed and transferred as well as how personal data should be handled. This will also help Community Councils meet their obligations under Data Protection legislation.

Managing Records

Community councils create, receive, use, and manage a variety of information in the course of their business. These will include core records, such as agendas, minutes of meetings and supporting papers. Other records such as correspondence, planning information, reports, financial transactions, survey data and administration information will also be generated and need to be managed.

There is a strong public expectation that democratically made decisions affecting citizens are properly documented and managed. Accordingly, each community council must:

- Create and maintain adequate records that meet the requirements of the Highland Council's [Community Council Scheme of Establishment](#)
- Document which 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 kept. This document should be reviewed and approved by the community council annually. Suggested template is provided at Appendix 1.
- Ensure that all records of the community council are retained for at least the retention periods required by the Highland Council as set out at Appendix 2.
- Ensure that electronic copies of agenda, meeting papers, minutes and annual accounts are transferred to the custody of the Highland Archive Service routinely and comprehensively. This should be done prior to each full Community Council election. Advice on this is given at Appendix 3.
- Ensure that their secretary and treasurer are aware of their responsibilities around managing the records of the community council.
- Ensure that all community council records that contain sensitive or personal data are securely destroyed when they are no longer needed.
- Document the date and authorisation of the destruction of community council records in a register that can be made available to the Highland Council upon demand. A suggested template is provided at Appendix 4.

When an individual ceases to be a community council officer, 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 officers should not retain any information relating to their work with the community council when they are no longer a part of it.

Protecting records

Of particular importance is the need to protect records, especially any records which contain sensitive or personal data. Community council officers 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 form, suitable controls should be in place to protect those records, and the information they contain, from accidental access. Various controls can be used such as:

- All folders should be password protected when storing information on home computers. Please note passwords should be removed prior to transfer to Archives.
- Create an alternative email address for community council business and ensure passwords are not shared.
- Use lockable storage to store any community council records, particularly those which contain sensitive or personal data.

If a community council officer suspects that information within their possession may have been accessed inappropriately, they should report their concern to the community council secretary or chair to ensure that appropriate action can be taken.

Managing Personal Data

Community Councils are subject to UK data protection legislation which is made mainly under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Community councils will process personal data. Personal data is any information that can identify a living individual. 'Processing' is an all-encompassing term: it means collecting, storing, sharing, managing, and disposing of personal data (basically doing anything with it).

The UK GDPR provides a governance framework which is based on seven principles. These principles guide organisations in how they collect and use personal data. The seven principles relate to:

- Lawfulness, fairness and transparency, organisations should only process personal data lawfully and in a fair way. We must tell people very clearly what we intend to do with the personal data we collect about them.
- Purpose Limitation, personal data should be collected for specific, explicit and legitimate purposes. If we have collected personal data and told the individual what we will do with it, we can't use the information for another purpose simply because we hold it.
- Data Minimisation, collected personal data should be adequate, relevant and limited to what is needed. We should only collect the personal data that is required for the task.
- Accuracy personal data must be accurate and, where necessary, kept up to date. Reasonable steps should be taken to rectify any data that is found to be inaccurate. Any personal data we hold should be routinely reviewed to ensure it is accurate.
- Storage Limitation personal data should not be kept in a form which allows individuals to be identified for any longer than is necessary for the purpose for which it was collected. Systems and processes should be designed to delete personal data as soon as it is no longer needed. This might mean that parts of records are deleted at different times.

- Integrity and Confidentiality personal data should be protected against unauthorised access, accidental loss, destruction or damage. Both physical and technical controls should be used as appropriate.
- Accountability organisations must take responsibility for how they handle and process personal data and should ensure that there are appropriate measures and records in place to demonstrate compliance.

Notification to ICO

Organisations still need to register annually with the Information Commissioner, but they will no longer need to tell the Commissioner exactly what they are processing through the process of notification. This information should be set out in the Privacy Notice(s).

Fees are still subject to agreement by Parliament; however it appears that the fees for registering are going up to £40 however if it's done by direct debit, £35 will still apply.

Privacy Notices Data Protection Legislation requires that if an organisation is collecting personal data, then they need to tell people what they are using it for. This is done through a Privacy Notice which sets out how you are going to process the data and how you will deal with it. This needs to be shared with anyone whose data you start to hold to ensure they know why and what you are using their data for.

A privacy notice ensures that people understand why their personal data is needed, and how it will be used. Providing clear information about this ensures that individuals are not surprised, and don't feel that their data has been used inappropriately.

Data Protection Legislation requires privacy notices to be clear, easily available, and concise. They must inform individuals of:

- Who the data controller is, and how to contact them
- Why the personal data is needed, and how it will be used
- Whether the personal information will be shared, and with whom
- How long the data will be kept
- Whether the data will be used for profiling or to make any automated decisions (i.e. decisions that are made without human intervention)
- How to make a complaint

The privacy notice must be in language that could be understood by a child.

The Council is publishing privacy notices on its web site to describe the different purposes it has for processing personal data. An example is provided at Appendix 5.

Further Information

The Council's Data Protection Officer can provide advice and or facilitate training on any data protection matters if required. Please contact him with any questions at: dpo@highland.gov.uk

Appendix 1: Template for recording general principles of record keeping

Record keeping responsibilities		Contact Details	
Chair			
Secretary			
Treasurer			
Other Community Council Members 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
<i>Minutes, agenda & meeting papers</i>			Main council, sub-groups and joint meetings with other bodies
<i>Accounts</i>			Annual Statement of Accounts
<i>Payments</i>			Cheques, invoices & expenses
<i>Bank account management</i>			
<i>Newsletters</i>			
<i>Surveys</i>			
<i>Consultation responses</i>			
<i>Membership / contact lists</i>			
<i>Official correspondence</i>			
<i>Event planning</i>			
<i>Grant records</i>			
<i>Constitution, standing orders</i>			
<i>Election records</i>			
<i>Annual Report</i>			

Appendix 2: Advised Record Retention Periods for Community Council Records

Record Types	Retention Requirements
Core committee records (to include constitution, standing orders, approved minutes, agenda, supporting reports and annual accounts)	Retain <u>Permanently</u> <i>Community councils must transfer these records to the Highland Archive Service prior to each community council election (see appendix 3 for instructions)</i>
Newsletters	
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
Projects (including campaigns)	Project closure + 2 years (small scale) or 10 years (large scale), then REVIEW
Surveys ; admin, preparation & <u>responses</u>	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	<i>For advice on EU funding record retention requirements contact the Council's European Affairs Team at: europe@highland.gov.uk</i>
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: Instructions for Transferring Community Council Records to Archive

Secretaries should ensure all agendas, meeting papers, minutes and annual accounts are transferred to the Highland Archive Service prior to each full Community Council election (every 4 years).

Records may be transferred to the Highland Archive Service by contacting: archives@highlifehighland.com for further details. This includes records in any format, such as paper or electronic. Secretaries coming across any "historic" Community Council records should also ensure these are passed to Archives.

You must ensure that any electronic records are in a good structure with accurately named folders and files. Any password protection on files must be removed as the Highland Archive Centre Staff need to be able to review the records.

Appendix 5: Privacy Notice

XXXX Community Council Example Privacy Statement

(to meet the requirements of the UK General Data Protection Regulation (UK GDPR))

XXXXX Community Council holds residents' contact details, with their consent, within password-protected databases (The WHAT).

The purpose for holding and using the contact details to communicate is both to inform and to seek views from residents. The purpose is a lawful public task for a community council to undertake in its legal obligation to ascertain and co-ordinate views of residents and to inform residents. Personal data may also be held, with consent, for other community activities that XXXXX CC considers appropriate. (The WHY)

The personal data held is not shared with any third party without specific consent. (DETAIL of SHARING)

Residents have the right, at any time, to access their own personal data for checking and updating and to request immediate removal of their data. Personal data may include email addresses, phone numbers and addresses but no other information. (RIGHTS)

Access to the data is restricted to the Chair, Secretary and Treasurer of XXXXX CC and [include details of other people who may process data for your community council] Personal data will be held only for as long as the consented purpose continues. (HOW LONG)

Within the meaning of GDPR, the Data Controller is XXXXXX Community Council which can be contacted through XXXXXXXX on XXXXXXXX (DATA CONTROLLER)

If you are unhappy with the way we have processed your personal information, you can contact the Information Commissioner who is the supervisory authority:

Information Commissioner's Office Wycliffe House
Water Lane Wilmslow Cheshire SK9 5AF
Tel: 0303 123 1113

<https://ico.org.uk/global/contact-us/> (WHERE COMPLAINTS CAN BE MADE)

ONCE COMPLETED PLEASE REMOVE COMMENTS IN RED

Document Control

Prepared By	Trevor Nicol, Records Manager
Original Authorisation	Philip Mallard, Information & Records Manager Miles Watters, Data Protection Officer
Next Review Date	

Document Revision

VERSION	DATE	AUTHOR	UPDATE INFORMATION
V01	05/12/2018	T Nicol	
V02	10/12/2018	T Nicol	Detail added on registering with ICO and advice on privacy notices
V03	01/02/2019	T Nicol P Mallard	Paragraph numbering added; document control and document revision details moved to beginning of document
V04	13/09/2023	M Watters	Data protection section updated
V05	13/09/2023	T Nicol	Amendments incorporated and appendix added for transfers to Archive
V06	21/09/2023	T Nicol	Final amendments incorporated