








DATA PROTECTION AND GDPR COMPLIANCE

Introduction

The Data Protection Act 2018 (alongside UK GDPR) governs the use of personal data, which ensures the fair and proper use of people's information and their right to privacy. It imposes important obligations on any persons or organisations, including Community Councils, which acquire, store, use or deal with personal data either electronically or within certain paper records.





The Data Protection Principles

The Act sets out some basic rules regarding processing personal data, known as the Data Protection Principles. These are –

-  **Principle 1:** Data must be processed fairly, lawfully and transparent;
-  **Principle 2: Purpose Limitation** Data must be obtained for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes;
-  **Principle 3: Data Minimisation** - Data must be adequate, relevant and not excessive;
-  **Principle 4: Accuracy** - Data must be accurate and kept up to date;
-  **Principle 5: Storage Limitation** - Data must not be kept longer than necessary;
-  **Principle 6: Accountability** - Data must be processed in accordance with the data subject's rights;
-  **Principle 7: Integrity and Confidentiality (security)** - Appropriate technical and organisational measures must be taken against the data's unauthorised or unlawful use and their accidental loss, damage or destruction.

Data Subjects' Rights






The Act gives important rights to data subjects, including the right –

-  To be informed that their personal data is being processed by the data controller;
-  To be given access to their personal data;
-  To require their personal data not to be used for direct marketing purposes;
-  To require the data controller to stop any processing of their personal data which is causing substantial and unwarranted damage or distress.

Complying with the Data Protection Act

Community Councils must comply with the Data Protection Act because they process personal data as defined under the Act. For example, it is likely that the Secretary of Community Councils will hold electronic records of contact details of its members, of some local residents and of elected members or employees of the local authority. These may be within databases, Minutes of meetings or in correspondence.

In order to comply with the Act, Community Councils should take the following steps:

-  Nominate someone as the person responsible for data protection.
-  If collecting personal data from individuals, you should explain the purpose for which the data is being collected as well as giving them the name of the Community Council and the name of the person nominated as being responsible for data protection.
-  Ensure that personal data are properly protected – if data are stored electronically, ensure that they are password-protected and (in sensitive cases) encrypted. If they are stored manually (e.g. a paper filing system), ensure that the files are kept in a secure place.
-  Ensure that personal data are never disclosed to any unauthorised third party, whether accidentally or on purpose. Do not discuss personal issues in public or leave papers or computer files unsecured at home.
-  Periodically review the personal data that are held, making sure that they remain accurate and up to date – where necessary dispose of or shred data that are no longer needed

Most breaches are likely to simply require remedial action to be undertaken and would not be deemed to be criminal offences. Good practice in data protection is vital to building public trust in the organisation.

All enquiries should be e-mailed to the Chair in the first instance at the following address:

chair@auchtermuchtyandstrathmiglo.cc