Data protection briefing document - Community Councils

The legislation:
The General Data Protection Regulation (GDPR) is a, **EU law** that replaces the Data Protection Act 1998 (the 1998 Act). It is part of the wider package of reform to the data protection landscape that includes the Data Protection Act 2018 (the DPA 2018). The GDPR sets out requirements for how organisations, must handle personal data. Scottish Borders Council register Community Councils on a yearly basis with the ICO on your behalf. As of 31 December 2020, legislation is changed again, the 'UK GDPR' will sit alongside an amended version of the DPA 2018. The key principles, rights and obligations will remain the same.

It is critical when you work with personal data that you understand the new rules and rights being introduced and are aware of how these may impact the work you do each day.

The principles:
There are 6 data protection principles that must be adhered to when dealing with personal data. These state that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner. You must have a lawful basis for processing the data and you must inform individuals what you will do with their personal data.

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. You are not free to use personal data for a purpose different from the one communicated to the individual in a privacy notice. You must have a good reason(s) for collecting, using and keeping individuals personal data.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. You should only collect the information needed for the purpose.

4. Accurate and, where necessary, kept up to date. Every reasonable step should be taken to ensure that personal data, where inaccurate, is erased or rectified without delay. You must ensure that personal data is regularly reviewed and inaccurate data is rectified, where appropriate.

5. Kept in a form which permits the identification of individuals for no longer than necessary. You should have a time limit in place for the retention of all data, and ensure that it is applied.

6. Processed in a manner that ensures appropriate security of personal data. You must ensure that personal data is protected from unauthorised access, unauthorised or unlawful processing, accidental loss, destruction or damage using physical and technical measures. It is good practice to carry out regular audits of information held and shared.

Newsletter mailing lists:

1. Always use blind copy (Bc…) when emailing personal email addresses unless you have consent of all the individuals.

2. Carry out regular checks to ensure everyone on the list wants to receive the newsletter. If they do not, their personal data should be destroyed in a secure manner.

3. If publishing the newsletter on the internet you should ensure that any personal information i.e. names, addresses, telephone numbers, signatures and e-mail addresses should not be published unless either Community Councillors or Committee Members and representatives from other organisations have consented to the information being published. It is good practice to hold a list of individuals that have provided consent.

Minutes of Community Council meetings:
Members of the public are generally aware who their Community Councillors are and members of the Community Council, SBC Council Officers and representatives from other organisations e.g. Police may expect their names to be in the public domain. It is good practice that the Chair advises the meeting before starting that the minutes may be published with names and should anyone have concerns these can be considered.

If there is any reference to members of the public during such meetings it is advisable that their names should not be in the public domain i.e. neighbour disputes, criminal offences etc. If possible, it should be highlighted that should a member of the public who is attending a meeting makes reference to another individual relating to perhaps one of the above scenarios then it is advisable that they should be dissuaded from doing so. If there is reference to a planning application then it is considered reasonable that the address for the planning application can be disclosed as these are already published by the Council.

Requests for personal data:
If you should receive a request for personal data of individuals other than those which are already in the public domain you should not disclose this information without their consent or ensuring a mandate is in place. Be careful when a request involves children and young people's personal data.

The person requesting the information may not be who they state they are and you should therefore take a note of their name and telephone number and advise that you will pass the message on. If the person whose details they are requesting wishes to contact them then they will do so.