Data Protection and Elected Members

What are data protection regulations?

Data protection regulations in the UK are primarily defined in the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA). These laws govern how organisations and data controllers must handle people's personal data, ensuring information is used lawfully, fairly, and transparently.

From 2025 onwards, these rules were further shaped by the Data (Use and Access) Act 2025 (DUAA), which amends—but does not replace—UK GDPR and the DPA 2018. The DUAA introduces updates designed to make data use more practical and proportionate while maintaining strong protections for individuals' rights.

What is personal data?

Personal data is defined as information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

This means personal data is more than just names, and may not even include a name. Personal data now includes online identifiers (for example, your computer's ID) and biometric data (for example, fingerprint or retina).

Am I a Data Controller?

As an elected member you wear up to three hats when it comes to data protection:

1. When working on behalf of the council, the council is the data controller and you should comply with all data protection policies set out by the council, including attending training, by not complying **you** are opening the council up to enforcement action and fines up to £17 million.

2. When working on behalf of a political party (where relevant), the political party is the data controller and you should comply with all their data protection policies.

3. When working on behalf of your constituents in your ward capacity **you** are the data controller and are responsible for all the data you process as well as **being liable for all action against you for a breach of regulations and any fines imposed.**

What are my responsibilities as a data controller?

Whenever you process personal data you must comply with the 7 principles of the GDPR:

- If you hold other people's data, then your processing must be:
    - lawful (one of the legal bases must be identified, see below),
    - fair
    - and transparent (a privacy notice must be available)
- Processing must be for specific and legitimate purposes – you must only process for a good reason, and only for the reason you have specified
- Personal data should be minimised so you are only collecting what is absolutely needed
- You must take reasonable steps to keep the data accurate and up to date
- Data must not be kept for longer than is necessary
- You must ensure appropriate security measure are in place this includes physical security, electronic security and appropriate training
- You must be able to demonstrate accountability in accordance with the regulations

What are the legal bases for processing?

- Legal obligations
    - processing is necessary for compliance with a legal obligation to which the controller is subject.
- Public Task
    - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Performance of a contract
    - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Vital interests
    - processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Legitimate interests
    - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child
- Consent – Not to be used by a public authority in most circumstances
    - Must be explicit, specific and be able to be withdrawn at any time

How can I ensure I comply with the regulations?

Some of the information above is quite technical, especially the legal bases.

The Information Management team offers a short training course to make sure you know everything you need to know, please look out for these and attend.