Data Protection: Guidance for Community Councillors

As of January 2021, the UK General Data Protection Regulation (UK GDPR) has taken effect. This brings the EU GDPR into UK law following Brexit.

The UK GDPR / Data Protection Act 2018 places obligations on organisations to protect privacy and enhance individual rights. This guidance will assist you in understanding your data protection obligations as Community Councillors.

There is also helpful advice published by the Information Commissioner's Office (ICO), the national regulator: https://ico.org.uk/

Types of personal data

There are two kinds of data which are covered by data protection legislation: personal data and special category data. All personal data must be protected, but special category data requires additional safeguards. Both kinds of data are considered confidential, unless specified otherwise.

Personal data: any information relating to a person who can be directly or indirectly identified. This includes identifiers such as names, identification numbers, location data, online identifiers or any other information that identifies an individual.

Special category data: Information regarding racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health data; sex/gender, sex life or sexual orientation. This information requires additional protections.

Examples of personal information:

- Employee names disclosed as part of Employee Appeals
- Names and addresses of Planning Objectors

Examples of special category information:

- Details regarding employees' health, medical conditions and wellbeing
- Details regarding employees' trade union membership

Roles: Data Controller and Data Processor

The nature of the legal responsibilities you hold depends on whether you are acting as a Data Controller or a Data Processor in relation to any given data processing activity.

Data Controllers: decide how and why personal data is collected, stored, used and shared ('means and purposes of processing').

Data Processors: carry out functions on behalf of a Data Controller, usually in line with their instructions.

The Community Council may act either as a Data Controller or a Data Processor. When you are undertaking business with your constituents, you are acting as an independent **Data Controller**; it is likely that this will be the majority of your activities. There may, however, be circumstances where

you need to use/share personal data as instructed by East Lothian Council; in these cases you would be acting as a **Data Processor**.

Registration with the Information Commissioner's Office

As **Data Controllers,** Community Councils should pursue registration with the Information Commissioner's Office. There is a fee, however these are set in a tiered system that applies lower fees for smaller organisations. You can find out more at Data protection fee | ICO.

Data Protection Principles

In general, you need to keep the following in mind when you are handling personal information:

- Handle personal information in a fair, lawful and transparent way.
- Only collect personal information for specific and legitimate purposes.
- Only collect or share personal information that is relevant and limited to what is necessary.
- Personal information should be accurate and up to date.
- Don't keep personal information for longer than is necessary.
- Keep personal information safe and secure.
- Make sure you are able to **demonstrate** that you are handling information in a compliant way. This means keeping good records of when and how you use information, and what protections are in place.

Data Breaches

Sometimes things can go wrong, and data can go missing or fall into the wrong hands. As Data Controllers, Community Councils are responsible for ensuring that data breaches are identified and mitigated as quickly as possible. In some cases, you may need to report a data breach to the Information Commissioner's Office, or to the data subjects themselves. Failure to address data breaches appropriately could lead to significant financial penalties and/or other enforcement action by the ICO.

Even seemingly small breaches need to be reported and contained, for example sending a letter to the wrong address or leaving personal information out on a desk where others can see it.

In cases where a data breach poses a likely risk to the rights and freedom of individuals (including a risk to privacy), you have a mandatory 72-hour window to report to the ICO. In cases where the breach poses a high risk, you are required to report to the data subjects.

You are responsible for ensuring that you know how to recognise a data breach, and when to report it. You can find out more at: Personal data breaches | ICO.

Information Security

Good information security is essential to protecting personal information. Good practice includes:

- Housekeeping – don't keep emails forever.
- Save attachments to a shared working area and remove the content from your email.
- Avoid using names and other personally identifiable information when you can.
- Measure twice, cut once – address autocomplete and similar names.
- Never store passwords in your email.

- Remain aware of your environment.
- Use lockable storage to protect paper records.
- Keep copies to a minimum.

Requesting information on behalf of constituents

When representing your constituents, you may need to access their personal information held by the Council. In this situation, you must get the consent of the individual to allow the Council to share this information with you. You can do this by asking the individual to sign a consent mandate; a template can be requested from the Data Protection Officer at dpo@eastlothian.gov.uk.

Contact the Council's Data Protection Officer

The Council's Data Protection Officer is Zarya Rathé, Team Manager – Information Governance. She can be contacted at dpo@eastlothian.gov.uk or on 01620 827 989.

The table below provides some examples of Controller vs Processor responsibilities.

Controller responsibilities	Processor responsibilities
• Registering with the ICO • Issuing Privacy Notices to individuals when collecting their personal data • Reporting breaches to the ICO within 72 hours • Keeping a register of processing activities • Issuing and maintaining consent records • Responding to requests for information from individuals (Subject Access Requests) • Keeping data safe and secure • Abiding by the Data Protection Principles Visit https://ico.org.uk for more information.	• Abiding by any data sharing arrangements • Undertaking relevant training • Keeping data safe and secure • Abiding by the Data Protection Principles