Data Protection & Community Councils

The purpose of providing you with this document is to familiarize you with data protection and the General Data Protection Regulation (GDPR), and to assist your community council comply with your data protection obligations.

Complying with data protection and GDPR law is the responsibility of the community council, adopting the policy documents (attached) will hopefully help you ensure compliance. However, they are **guidance** documents, not tablets in stone, and I would encourage all community councils to consider the contents and make any changes as you see fit for the purpose of improving or amending the **Data Protection Policy (3)** and the **Community Council Social Media Policy (5)** to suit your particular community council.

If you wish further information or clarification on a point; feel free to contact me with your enquiry.

Regards

Vincent McCulloch
Community Council Liaison Officer
East Renfrewshire Council
Eastwood Park
Giffnock G77 6UG

This document contains the following information

1. General Data Protection Regulation (GDPR), background Information.
2. Data protection - Community Council Guidance Notes
3. **Data Protection Policy for Community Councils**
4. Social Media and Community Councils – Notes and guidance
5. **Community Council Social Media Policy**
6. Community Councils Privacy Notice
7. Sources for additional information on data protection and GDPR

(1) General Data Protection Regulation (GDPR), background Information.

On May 25, 2018 the European Union General Data Protection Regulation (GDPR) came into force. This is arguably the most important change in data privacy regulation in 20 years. It is designed to harmonize data privacy laws across Member States; to protect and empower all EU citizens' data privacy; and to reshape the way organizations across the EU approach data privacy. Although the UK is leaving the EU, the data protection regulations will remain in place through the data protection Act 2018 and future planned legislation.

One of the most important aspects of the GDPR is accountability. The new legislation places an onus on organisations to know and understand the risks their handling of personal data creates, to mitigate those risks, and to demonstrate they have done so.

Under the updated Personal Data definition, which reflects changes in technology, a person's name, their addresses, bank details, medical details and IP addresses, which relate to an individual's private, professional and public life, should all be protected

The Act regulates the processing of personal data. "Processing" means acquiring data, storing it, amending or augmenting it, disclosing it to third parties, deleting it – i.e. doing anything with it at all.

1. **What it Aims to Do**

   Intended to reinforce data protection for individuals in the European Union (EU), the regulations give control of personal data back to the citizens and clarifies the regulatory environment for international organisations. The GDPR also addresses the exporting of personal data outside of the EU.

2. **Controllers**

   Controllers are the people who say how and why personal data is processed. Under the GDPR they have new obligations where a processor is involved and must ensure they comply with the regulations.

3. **Processors**

   The processor acts on the controller's behalf to process personal data. The GDPR places them under specific legal obligations requiring them to maintain records of personal data and processing activities. If a breach occurs then a processor now has more legal liability, if they're responsible for it.

4. **What is Personal Data?**

   If the information you process fell under the scope of the Data Protection Act, it's safe to assume that it will also fall under the new GDPR. This includes the keeping of HR records and customer lists which state an individual's name, address, email and phone number amongst other things.

5. Detailed Definition of Personal Data

The GDPR also presents a more detailed definition of what personal data is, reflecting the changes in technology, stating it's any information relating to an individual's private, professional or public life. For example, the new regulations identify IP addresses and social media posts, as data that needs to be protected.

6. Holding Data

The regulations apply to both manual filing systems and automated personal data. If the data is kept under a pseudonym then it can also fall within the GDPR depending on how easy it is to identify the individual concerned.

7. Special Category Personal Data

When referring to 'sensitive category data' the GDPR detail it's 'special categories of personal data'. These are roughly the same as those in the Data Protection Act (1998), but also include genetic data and biometric data processed to uniquely identify an individual. Data related to criminal convictions is not included, but safeguards for its processing are in place under the Law Enforcement Directive.

"Special category personal data" means information regarding such things as an individual's racial or ethnic origin, political or religious beliefs, physical or mental health, sexual life and commission of a criminal offence. Special rules apply to special category data and Community Councils should seek advice if they hold any special category data (other than that which is in the public domain such as the political affiliation of local elected members or the denominations of clergy).

8. Collected

Data should be collected for specified purposes and not processed beyond it with exception of archiving purposes, scientific or historical research or statistical reasons.

9. Accurate,

Data should be accurate, adequate for and limited to what's necessary for the purpose. Inaccurate data should be erased or rectified with regard to the original purpose of the data's collection.

10. How its kept

To protect the rights of the individual, appropriate technical and organisational measures should be used when keeping data, and kept no longer than is necessary for the purpose.

11. Processing

The processing operation should be conducted in a way that protects against unlawful processing, accidental loss, destruction or damage.

12. The Rights

The GDPR strengthens some of an individual's rights that existed under the DPA, while also introducing new ones.

- **The Right to be Informed -** This covers your obligation to provide 'fair-processing' information, usually through a privacy notice and emphasises the need for transparency between the organisation and individual over how personal data is used.

- **The Right of Access -** Individuals have the right to obtain confirmation that data is being processed, access to their data and any other supplementary information. This is typically covered in the privacy notice (an example is attached) and is similar to existing rights in the Data Protection Act.

- **The Right to Rectification -** If the data is inaccurate or incomplete then an individual has the right to rectify the situation. If that data has been passed onto a third party, the individuals must be informed, where appropriate, and updates passed on.

- **The Right to Erasure -** Also, known as the right to be forgotten, it enables individuals to request their personal data is either removed from a database or deleted. This can occur when consent is withdrawn, the data is no longer necessary for the original purpose, it was unlawfully processed, to comply with a legal obligation, the individual objects to the process, or there's no overriding legitimate interest in continuing.

- **The Right to Restrict Processing -** Similar to the rights of the Data Protection Act, individuals have the right to block or suppress the processing of personal data. When restricted you're permitted to store personal data, without further processing, and retain enough information to ensure the right is respected in the future.

- **The Right to Portability -** This allows an individual to obtain and reuse their personal data for their own purposes, enabling them to move, copy or transfer the data from one electronic environment to another, safely.

- **The Right to Object -** Individuals can object to the processing of personal data for a number of reasons including for direct marketing or the processing of information for scientific or historical research and statistical purposes.

13. **Requirements -** Let's explore the requirements set out under the new GDPR:

    Lawful Processing - For processing of personal data to be considered legal under the GDPR, you need to identify and document a legal basis as it could affect an individual's rights. The lawful bases for processing are set out in Article 6 of the GDPR and are detailed below. At least one of these must apply whenever you process personal data: (*The legal basis which is used by CCs will mainly be **consent***)**.**

    (*The legal basis for the processing of Special Category Personal Data, are detailed in article 9 of the GDPR*).

    (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
    (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
    (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
    (d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

14. **Consent –** (This is the main lawful reason for Community councils collecting personal data). Consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes. As the regulations require a clear, affirmative action; silence, inactivity and pre-ticked boxes don't count. The consent should be recorded so it can be verified and individuals have the right to withdraw consent at any time, a right they must be informed about, usually in a privacy notice/statement. This notice will also detail other rights of data subjects. (***An example privacy notice is attached to this document).***

15. **Transfers out of the EU -** There are also restrictions on the transfer of data outside of the EU to third countries or international organisations, to ensure the level of protection offered by the GDPR isn't undermined. It can only be transferred if it complies with conditions set out in Chapter V of the GDPR or the Commission decides that the country or organisation guarantees an adequate level of protection.

16. **Accountability -** Under the GDPR there is a new requirement for accountability, with what was previously implicit in the DPA, now explicit. Organisations are expected to put in place comprehensive governance measures, such as privacy impact assessments and privacy by design, which are recommended by the Information Commissioner's Office (ICO) and are now legally required in some circumstances. Although organisations will already have these measures in place, more policies and procedures could be required.

17. **Breach Notification -** It is now the duty of an organisation to report data breaches either to the relevant supervisory authority, or in some instances, to the individuals affected, as they can be held accountable if the breach occurred because of a lack of inappropriate internal controls. A data breach is an event that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

18. **Results of Non-Compliance -** If an organisation doesn't comply with the new regulations they can face a number of penalties which are dependent on several factors including the duration of the infringement, the number of individuals affected and the level of impact. In severe cases of non-compliance, organisations could be fined up to 20 million euros or 4% of the total annual turnover, whichever's highest.

Information Commissioner - is the independent regulator responsible for ensuring all organisations comply with the Data Protection Act. Organisations are required to notify the ICO of how they process personal data and if they breach the Act. The Commissioner has been granted enforcement powers regarding non-compliance, these include the ability to issue information and enforcement notices, impose large fines, and bring a criminal case against an organisation.

(2) Data protection - Community Council Guidance Notes

All Community councils in East Renfrewshire will hold personal data, and have the responsibility of complying with data protection law. The Community Council is the controller of this personal data, it is the Community Council who say how and why personal data is processed. Community Councils are **not** obliged to have a designated data processor; however, they may wish to appoint one of their members to undertake the task and responsibilities of a data processor.

> ***Role of a Data processor***
> *The processor acts on the controller's behalf to process personal data. They are required to maintain records of personal data and processing activities.*

What Personal Data do Community Councils hold?
Anything which state an individual's name, address, email and phone number amongst other things.

Examples of personal data held by Community Councils

CC members – ERC elected members, ERC council workers, employees of other organisations, members of the public, suppliers of goods, members of other local organisations etc. Social media posts are also data that needs to be protected.

It is important that an audit of personal data held by the CC is carried out, in the first instance this will give an opportunity to consider if the personal data held is actually relevant, if it is not, dispose of it in a suitable way. It is against the regulations to 'hold on' to someone's personal data for some unspecified future use. Make sure that all CC members check if they hold personal data, (phones, computers, paper copies etc.) And ensure that they provide these details to the cc member carrying out the audit. **(An example personal data audit sheet is below).**

> **Note** – Anyone who has an email account or receives texts will probably be very used to clearing out emails and texts that they do not need, usually because they are outdated. CC members just need to apply the same scrutiny to items relating to the CC.

Audit of Personal Data Held (Example)

Description of Data	Location of Data	Action	Date of Action	Notes
Names and contact details of **former** CC members	Paper & digital (email)	Delete	19/5/2018	Not required
Names and contact details of ERC Councillors	Paper & digital (email)	Retain	19/5/2018	Required (this information is also published and is in the common domain)
Name and contact details of Residents Association	Paper	Delete	19/5/2018	Person is no longer the secretary.

Secretary				
Names and contact details of Scottish Water communications officer	Digital (email)	Retain	23/5/2018	Still relevant as infrastructure works ongoing. (this information is also published and is in the common domain)
Names and contact details of Local resident complaining about potholes.	Digital (email)	Retain	23/5/2018	Although still relevant, consent is required prior to forwarding email to Cllrs and ERC Roads.

(3) Community Council Data protection Policy

Policy statement
This policy sets out the Community Councils approach to managing personal data in accordance with the requirements of the relevant Data Protection Acts (including the changes introduced by the General Data Protection Regulation (GDPR)– May 2018).

Implementation
The Community Council having approved this policy at a meeting held on (*insert date of meeting)* will incorporate an annual action plan for information governance development and compliance, including data protection. The plan will outline key tasks, outcomes, accountabilities and progress.

All CC members have responsibility for data protection and must:

Read, understand and follow this policy and any associated procedures that relate to the use and handling of personal information in the course of their voluntary work as a member of the community council;

Undertake data protection training and ensure they have a clear understanding of their responsibilities in using and handling personal information;

The community council will uphold the 6 principles regarding personal data

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

To ensure compliance with these principles, the community council will undertake the following actions.

Action Points

- Only use the personal data we hold for Community Council business.

- Inform data subjects in writing that their personal data is held and the purpose of holding it and if they consent to the CC continuing to hold it for a specific (and stated) purpose, this is done through the use of a privacy notice (an example privacy notice is attached to this document).

- Only collect information we need.
- Follow agreed retention rules for the data that we hold. We will review the data annually.
- We will have reasonable controls in place to keep personal data secure: (i.e. - use 'Bcc' field in emails were appropriate; keep papers secure, etc.
- Understand security arrangements of websites/systems if used to collect/store personal data
- If sharing personal data with other organisations, document arrangements so those involved know why the information is being shared, and how it is shared.

The community council will review this policy annually for the purpose of ensuring that members have adhered to the policy, and to make improvements if there have been issues with regards to its implementation.

(4) Social Media and Community Councils – Notes and guidance

The explosion of online social media networks and the ever-increasing sophistication of mobile devices to allow immediate access to view and update these sites has transformed both personal and professional communications and radically altered the landscape of the traditional communication channels.

New technologies are enabling ordinary people to build new networks, share and comment on information and access content as never before.

It is important that community councils can deliver messages to target audiences effectively using platforms they are most comfortable with, but they should ensure that users can understand and identify with what is said and where appropriate, choose to act on it or share our messages with others.

Community councils recognise the importance of social media networking sites as a significant tool to supplement more traditional communications channels and should utilise these platforms to keep members and other stakeholders informed of our activities, plans, key messages and vital information. Where appropriate, the community council will also support members to use social media platforms to optimise opportunities to promote the CC in the correct manner and in accordance with the community council's aims and objectives.

Social media will be used by the community councils as a concise and fast platform to inform and engage with the public and increase the online presence of the community councils. It can also be used as an additional tool to encourage participation and engagement as well as a channel to market key community council information.

GDPR does not apply to individuals using social media for their own purposes, but it does apply to organisations that use social media in the following ways:

- Posting personal data on a website
- Downloading and using personal data from a website
- Running a website which allows others to post comments or other content about people

This means that if an organisation posts on a social network or a blog, or uses personal data from a social networking site, they are usually subject to data protection laws.

If a community council runs an online forum or comments section, then they have a responsibility for the content posted. This includes a duty to take reasonable steps to monitor and moderate the content posted. Reasonable steps must be taken to check the accuracy of any personal data posted by a third party. While it may be unreasonable to moderate every comment, there would at least need to be an option to report problematic posts.

Determining who in a community council can say what, and when they are representing only themselves or the community council is difficult. While it is generally recommended to keep personal and community council social media presence separate, this is not always possible. It is therefore important for community councils to have clear policies on social media use by community councillors.

What should be included in a social media policy?

You may want to include the following points in your social media policy:

- The risk of defamation
- The reputation of the community council
- Handling negative comments
- Monitoring community councillors posts
- Monitoring posts from members of the public.

Community councillors may be subject to criticism for posting comments online that may damage the community council's reputation. Therefor the 'rules, standards and etiquette' for posting social media comments needs to be communicated to all community councillors.

It is also advisable to use a disclaimer that any opinions expressed are personal and do not represent the views of the community council.

(5) Community Council Social Media policy

This policy is intended to provide guidance on the use of social media by the community council and will outline the standards required by members when using community council social media sites. This will hopefully ensure that the community council's social media use is compliant with data protection and GDPR laws.

RESPONSIBILITIES

1. The community council will manage and maintain the social media accounts and post updates and news on them, share information and respond to enquiries that come in via these platforms.

2. Failure to manage our social media channels correctly has the potential to damage our reputation. Poor management or understanding of social media tools can lead to social media group members posting improper or incorrect information on social media sites.

3. Only designated members will be permitted to update official social media sites on behalf of the Community council. Any member or members can make content suggestions to the community council and they will post news, photos and events on behalf of members as appropriate.

4. Members using social media accounts on behalf of the Community council have a responsibility to provide useful and engaging content to the public, which portrays the community council in a professional manner and reflects our aims and objectives.

5. The CC will monitor social media accounts and produce regular reports, which will be evaluated with an aim to develop our online interaction with a range of audiences.

6. Any requests to use social media platforms on behalf of the community council should be directed in the first instance to a community council meeting so that members can discuss plans and provide a level of support to ensure best practice.

7. Members should not create any community council social media sites without gaining appropriate agreement at a committee meeting where it has been fully discussed and agreed by members.

8. Members must not engage in criticising or arguing with fellow members or the wider public on social media platforms.

9. Members must not make defamatory statements about the community council, individuals or other organisations online.

10. Posting content, which could be deemed to be unlawful, abusive, obscene or harmful, which includes sharing or posting links to such content is unacceptable.

11. Any concerns about this type of action from members should be raised at a committee meeting at the earliest opportunity.

12. Using social media to bully, or appear to bully or harass, a member or any another individual is not acceptable.

13. Members must not comment on or disclose any confidential or sensitive information about the community council.

14. Posting any information or content that is copyright protected, without the permission of the copyright owner is also forbidden.

15. There is a risk to members from the misuse of any social media sites. Inappropriate content or posts may give grounds for complaint against the members and/or the community council. If in any doubt, discuss with the Secretary/Chairperson who will be able to give appropriate guidance.

16. Members should not write a blog in an official capacity i.e. representing the views of the community council without the permission of the community council. If, however, they give a personal opinion as an experienced person in a particular field, they must state that it is solely their views and not the view of the community council.

17. If you are a member who believes that you are being harassed, bullied or victimised as a result of another member's post to a social media site, which you think may be in breach of this policy, you should make the chairperson aware as soon as is practically possible.

The community council will review this policy annually for the purpose of ensuring that members have adhered to the policy, and to make improvements if there have been issues with regards to its implementation.

(6) Community Councils Privacy Notice (Community council Members)

Who will process your information?
The personal information you give to us in relation to Xxxx community council and any other personal information we hold about you in this context will be processed by Xxxx community council,

Why do we process your information?
You are giving us your personal information to allow us to process data as you are a community councillor or have been proposed for membership of Xxxx community council. We also use your information to contact you by post, email or telephone in respect of community council related matters, and to maintain our records.

What is the legal basis for us to process your information?
We process your information as you have consented to being a member of Xxxx community council. We have a duty under the ERC scheme of establishment for community councils to keep you informed of matters relating to the organisation and effective functioning of the community council.

Who is your information shared with?
Your information will be shared with other members of Xxxx community council, and with East Renfrewshire Council.

How long do we keep your information for?
We only keep your personal information for the period of your membership of the community council. Your information will be destroyed under confidential conditions after this period.

Your rights
You have the right to:
1. Be informed of the community council's use of your information
(This notice is intended to give you relevant information to meet this right).
2. Access personal data held about you
3. Request rectification of your personal data
4. Request that the Community council restricts processing of your personal data
5. Object to the processing of your data
6. Ask us to delete your information –

Further information about these rights and how you can exercise them can be obtained from the Community Council's general document on Data protection and from the Information commissioner's website.

Complaints

If you have an issue with the way the community council handles your information or wish to exercise any of the above rights in respect of your information you can contact the secretary of Xxxx Community Council. Contact details are below

You also have the right to complain directly to the Information Commissioner's Office (ICO). Contact details are below.
While you can go directly to the ICO, the community council would welcome the opportunity to address any issues you have in the first instance.

Contact Information
The Secretary
Xxxx community council
44 The Street
Email Xxxxcommunitycouncil@aprovider.com

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

https://ico.org.uk

(7) Sources for additional information.

https://ico.org.uk/for-organisations/local-government/local-gov-gdpr-faqs/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

https://www.eugdpr.org/

http://scvo.org.uk/projects-campaigns/datawareness