APPENDIX 4

GDPR – Top 12 Tasks for Community Councils

Community Councils will receive and use information relating to identifiable, living individuals. This is known as "personal data". Your organisation is also known as a "data controller" as you are processing personal data.

The purpose of this briefing note is to highlight the key changes being introduced by the General Data Protection Regulation (GDPR) and the new Data Protection Act 2018 which may apply to your Community Council. This legislation is enforced by the Information Commissioner's Office (ICO).

Task #1: Notification. Data Controllers must pay a fee annually (starting at £40) to the ICO, unless an exemption applies. Not-for-profit organisations are not required to pay a fee in some cases, however it is recommended that you carry out the online assessment to establish whether payment of a fee is required. It can be found here: https://ico.org.uk/for-organisations/data-protection-fee/

Task #2: Responsibility for Data Protection. You may have heard that some organisations, such as Fife Council, are required to appoint a Data Protection Officer (DPO). It is unlikely that Community Councils will require a DPO however you may wish to consider nominating someone as the person responsible for data protection matters.

Task #3: Record of processing activities. Many organisations are now required to keep what is known as a "record of processing activities". It is unlikely that Community Councils will be required to keep such a record. However, you may wish to document what records will be created or held by your Community Council and how they will be stored (eg by email; in paper files etc). It is important to know what personal information you are using and why.

Task #4: Privacy Notice. Every Data Controller must tell people how their information is used and why. This is known as a privacy notice. Data Controllers are now obliged to tell people much more information and it must be communicated in a clear, concise manner. Fife Council has opted for a layered approach. We have placed a high level corporate notice online: www.fife.gov.uk/home/privacy-policy and Services have prepared their own privacy notice to sit under this. Finally, we are arranging for all forms, letters etc to be updated to refer to these notices.

This is clearly too detailed for your purpose. We have prepared a template for completion by Elected Members and these have been uploaded to Fife Council's website. This is attached at Appendix 4 (a). You may wish to consider adopting this or a similar approach and arrange for it to be uploaded to your Community Council website, if you have one. Once you have a privacy notice in place, you then need to consider how you can communicate this to individuals when they initially contact you. For example, do you have any forms or letters that can be updated with either this notice or the weblink? Or can you put up a poster.

Task #5: Data Sharing. If your Community Council routinely shares personal information with another organisation then you may require to formalise this arrangement through a Data Sharing Agreement or Information Sharing Protocol. In any type of data sharing, it is recommended that you keep a record of what information is shared, with whom and why.

Task #6: Consent and Processing Personal Data Lawfully. You must only process personal data where you meet one of the lawful conditions for doing so. Public authorities are no longer allowed to rely on consent however Community Councils can do so. The rules around consent have changed and you must ensure that consent is clearly obtained at the outset with the individual "opting in". This may comprise a mandate signed by community council members confirming that they consent to the use of their personal information. This mandate could include a link to your new privacy notice (see Task #4 above). The ICO has published detailed Guidance on the use of consent together with a checklist and it can be found here: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent-1-0.pdf

Please note that consent can now be withdrawn at any time and you must stop using the personal data.

The ICO has also published an interactive guidance tool so you can work out if consent is the right legal basis for you. It can be found here: https://ico.org.uk/for-organisations/resources-and-support/lawful-basis-interactive-guidance-tool/

Task #7: Understanding some key principles.

- Only collect and use the minimum amount of personal data necessary to carry out the task.
- You can only use the personal data for the specific purpose it was collected for. You cannot then use it for another unrelated purpose.
- You must ensure that the personal data you hold is accurate. You should carry out periodic checks to ensure the data is still accurate and up to date.
- You must not keep personal data for any longer than is necessary.
- You must ensure that personal data is held and shared securely. For example, use locked storage to keep any paper records, particularly those containing sensitive or personal data.
- Ensure you consider data protection when considering new projects.

Task #8: Data Breaches. Sent an email containing personal information to the wrong person? Lost a paper file containing personal data? You now have to report data breaches (in certain cases) to the ICO within 72 hours of someone first becoming aware of the breach. It is true that the level of fines which can be imposed by the ICO have increased for a breach of GDPR or the new Data Protection Act. They also have other enforcement powers available. You should ensure that the individual identified at Task #2 is aware of the following guidance: https://ico.org.uk/for-organisations/report-a-breach/

Task #9: Subject Rights. You are probably aware that someone can request a copy of their own information (known as a Subject Access Request). This is still available under GDPR with a few changes. But there are a number of other rights available to individuals (some new, some available now) such as the "right to be forgotten". This means that individuals can request that you remove/delete all their information (but you do not always have to comply). It is unlikely that you will routinely receive these requests however it may occur. The ICO's Guide to the General Data Protection Regulation (see details below) contains a section on this.

Task #10: Marketing. The rules on direct marketing (eg by email) have not been changed by GDPR. If you undertake any form of marketing then the ICO has a self assessment tool available: https://ico.org.uk/for-organisations/marketing/

Task #11: Secure Storage. All your records must be stored securely. Paper records should be kept in locked storage and electronic files should be stored on secure drives, in the cloud or encrypted devices like a portable hard drive. Physically separate storage devices from other hardware. Back up data on a regular schedule, store backups off site securely.

Task #12: Records Retention. All your records should be kept for the right period of time and promptly and appropriately disposed of at the end of that time. For guidance on how long to keep different records for, see the Scottish Council on Archives Records Retention Schedules (SCARRS). This is a Scottish National Framework for local government records retention. A PDF of the combined schedules can be downloaded from http://www.scottisharchives.org.uk/scarrs/schedules . For further guidance on records retention, please contact the Council's Records Manager Meic Pierce Owen at: meic.pierceowen@fife.gov.uk

Further Information

We appreciate there is a lot of legally technical points to be considered. If we become aware of any detailed guidance for Community Councils then we will let you know. In the meantime, it is recommended that you begin to work on the above tasks if you have not already done so. We would also recommend that you read the ICO's Guide to the General Data Protection Regulation which can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

You may also wish to take your own legal advice on the impact of GDPR on your Community Council or contact the ICO directly. In the meantime, if you have a specific query then the Council's DP Team would be happy to share the Council's equivalent guidance or template or refer you to the relevant ICO Guidance. The Council's DP Team comprises: Fiona Stuart; Karen Welsh or Karen Berry at: dataprotection@fife.gov.uk

APPENDIX 4 (a)

Template Privacy Notice – for elected members

As a Fife Council councillor, I [elected member name] will use the information provided by you in order to represent your views and opinions and to help with any difficulties that Fife Council could help to solve. I am what's known as a data controller for this information. I am carrying out this role and using your information in order to fulfil a public function in the public interest.

The personal information that I gather and use includes your name, contact details and information relating to your query or consultation with me.

I will keep your information for [insert how long], then it will be securely destroyed.

I share your information with Services within Fife Council to ensure you are provided with help, advice or services that you are entitled to. I also share your information with my IT suppliers (via Fife Council) and with the Council's Members Service so they can provide support to me as an elected member of Fife Council [insert any other data sharing here].

In order to carry out the functions above, I may also receive information about you from Services within Council.

If you have concerns about the use of your personal data, please contact me in the first instance. If you remain dissatisfied, you may wish to contact the Information Commissioner's Office to raise your concern or complaint. The ICO can be contacted in writing at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or telephone: 0303 123 1113 or online: https://ico.org.uk/concerns/getting/.