

IT Update on Parish Websites and GDPR Issues – September 2019

This is the first of our occasional **KALC IT updates**, which we hope your council will find useful?

- This update refers to the latest GDPR updates issued by the **Information Commissioner's Office (ICO)** [<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/blog-three-top-issues-for-town-and-parish-councils>] and also a **KCC Parish Council website hosting** update.
- We have extracted the salient points for you and expanded where necessary. **Please Note** that this information does require discussion by your Council, and plans made to ensure compliance where necessary.

ICO GDPR Update:

Stacey Egerton, Senior Policy Officer, wrote on the 14 August 2019:

"The advent of the GDPR in May 2018 brought new data protection obligations for many organisations. Some of this presented a challenge, particularly for smaller organisations like parish and town councils, who we saw were keen to demonstrate their compliance but needed support to achieve this.

Now, well into the second year of the GDPR, it's clear that organisations have woken up to the importance of getting privacy right and the new rights that the GDPR delivers, with increased protection for the public and increased obligations for organisations.

But the focus is shifting to a new phase from basic compliance with the law, towards accountability and a real evidenced understanding of the risks to individuals in the way they process data and how those risks can be mitigated. We've seen evidence of good practice across the board, but we know there's a lot more to do.

My colleagues and I have been working extensively with town and parish councils to help them with their compliance. For example, we've carried out a lot of engagement work around the GDPR, speaking to more than 50 local councils to help address their concerns, identify pitfalls and gain a better understanding of how they are run.

As a result of this work, we're pleased to be launching a number of bite-sized resources which address the top three GDPR compliance challenges that we identified through the feedback we gathered from the sector."

The first comment to make here is to emphasise that the ICO is now moving from the 'start-up' phase of GDPR towards more accountability and **evidence** of a real understanding of what those data risks are for your Council, and how you might lessen them. As part of that evidence, KALC would encourage you to consider your Data Protection Officer's reports in a Council meeting so that it is recorded in the minutes. How you might lessen those risks depend upon your Council's own circumstances, but your Data Protection Officer should have already advised you of this.

The ICO then give a link to 'Own Devices':

That is, holding personal data on personal laptops or mobile phones and the use of non-council email addresses by councillors instead of the council system. We recommend you click on this link in order to download it: <https://ico.org.uk/media/for-organisations/documents/2615578/parish-councils-own-device-fact-sheet.pdf>

Here are the main points from that Fact Sheet:

- The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) don't say which email systems or devices should be used. **But if the use of personal email addresses and devices is something your council does, you should be aware of the risks and the council's data protection obligations and responsibilities.**
- Councils must ensure the confidentiality, integrity and availability of all personal data they hold, even if the data is being processed through personal email accounts or is stored on a privately-owned device.
- As a data controller, a council has obligations relating to the confidentiality, integrity and availability of all personal data it holds. This means that the council is accountable for any council business conducted involving personal data on any device or through any email account.
- If copies of data (such as email attachments) are stored on many different devices, there's an increased risk that it'll become out-of-date or inaccurate over time. There's also an increased risk that it'll be retained for longer than necessary, because it's difficult to keep track of copies.
- You may also find it difficult to respond on time to a subject access request if you have to search multiple devices or if you aren't aware of all the devices on which personal data may be stored.
- Councils must have 'appropriate technical and organisational measures' in place to prevent the personal data it holds being accidentally or deliberately compromised. This includes physical and organisational security measures and also cybersecurity. If data is shared around multiple devices this introduces more points of failure and vulnerability.

In essence, Councils must demonstrate that they are GDPR-compliant, and the use of personal email accounts and privately-owned devices may make this more complicated and will make it harder to satisfy the ICO's current phase: accountability and evidence.

We suggest you read the whole Fact Sheet as it contains further information for your Council to consider, along with a series of questions that will help you conclude regarding the use of personal IT equipment and emails.

The ICO then give a link to Data Audits:

Retention of information 'just in case' it could be useful doesn't mean it's necessary or proportionate to hold on to it. Councils could benefit by giving their records a good spring clean, deleting or destroying old data sets that have built up over time. Parish councils often don't have formal handover processes in place which ensures clerks who are moving on hand over relevant data to the new clerk – and delete or destroy the rest.

Does your Council have a Policy for handing over to new staff? Does your Council have a Data Retention Policy (see NALC LTN 40 – Local Council's Documents and Records)

KALC recommends that you download the Parish Councils Resource Pack in order to help you: <https://ico.org.uk/media/for-organisations/documents/2615588/parish-councils-resource-pack-201908.pdf>

The factsheets will guide you through the various points that your Council should consider.

The ICO then give a link to Data Sharing:

Councils struggle with knowing how to share data appropriately with services such as leisure centres. They worry about potential conflicts between different pieces of legislation and aren't sure whether to publish residents' names in council minutes, or how to redact them.

The ICO has published a 6-Step Guide here: <https://ico.org.uk/media/for-organisations/documents/2615580/parish-councils-six-steps-fact-sheet.pdf> This contains additional guidance and tools which will help your Council to deliberate and decide upon your appropriate action.

Here are the main points the ICO makes:

- There must be a specific purpose for sharing personal data. Before you share information with another organisation you should be clear on what the sharing is meant to achieve. You will need to record your purposes and specify them in your council's privacy information to individuals.
- To comply with GDPR you must identify and document an appropriate lawful basis for sharing the information. There are six lawful bases and no single basis is better or more important than the others – the most appropriate one for your council will depend on your purpose.
- Many of the lawful bases for processing depend on the processing being necessary. The sharing has to be more than just useful or standard practice for it to be necessary. If you can reasonably achieve the same purpose another way or by sharing less information, then the sharing won't be necessary, and your lawful basis won't be valid.
- Councils should only share the minimum amount of personal data that is needed to help your council achieve its purpose. Sharing more information than is needed may be considered excessive and in contravention of GDPR.
- Individuals have a right to be informed about the use of their personal data. It's also a key transparency requirement under the GDPR. When you collect the information from individuals, the GDPR requires you to inform them of certain information. This is known as privacy information. Even if you don't get the personal data directly from the individual concerned, you still must provide them with privacy information.
- The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles of GDPR. If you're sharing personal data, you'll need to evidence your compliance and justify your approach.

Documenting the purposes and lawful bases for your council's data sharing is a good example to demonstrate your accountability. If you regularly share data with the same organisation, then a data sharing agreement would be good practice to demonstrate your accountability.

Stacey Egerton concludes: *“Through steady engagement we've seen councils grow in confidence and by encouraging others in the sector to follow their lead, parish councils will be better placed to be compliant – and be less likely to face action by the ICO. It's important that **data protection remains high on the agenda** within the sector....“*

Parish Council Website Hosting Update:

For those 160 Member Councils who still use KCC (EIS) for their free website hosting, KALC attended a meeting recently and was informed that they cannot continue to fund the free website from 1st September 2020.

The current KCC EIS websites are not '*Web Accessibility Compliant*' and need a radical overhaul. The company that are managing the current website are developing a new template that will be compliant. However, there will be a cost to Parish Councils if they decide to use the new website from September 2020. We will be meeting the company shortly and will then provide more details on the cost of the new website and the template.

We are also in discussion with several other providers who already offer a service to Parish and Town Councils, including porting across your existing website, and so will distil further information to you in late September, along with other suitable advice.

For those councils that use a HugoFox website, you will be pleased to know that it is already compliant (see screenshot), although, having said that, they are currently undertaking a review to ensure their framework suits the latest guidance.

There are a few points to consider when judging whether your Website is '*Accessibility Compliant*'. As a Council, you might like to think about these two points first:

- When saving Word documents as pdf files, consider using the built-in Microsoft Print to PDF

This ensures that your PDF file can be read successfully by the built-in Microsoft Narrator, used by many partially sighted or blind people around the world.

It might be considered unreasonable to ensure all your existing documents are compatible with Narrator. Our advice, however, is to ensure important documents, like policies, etc., are made compliant and that all future PDFs are able to be played by Narrator.

- The colours you use, for text, shading, and especially text in boxes, are important. You are responsible for ensuring that these are '*Accessibility Compliant*'. Our suggestion is, in the first instance, that you contact your Web Provider to enquire further.

