**General Data**

**Protection Regulations**

**(GDPR)**

**A Quick Start Guide**

**For Parish/Town Councils**

****

***With thanks to Northants ALC***

**Introduction**

This Quick Start Guide will get you quickly on the journey towards compliance with the General Data Protection Regulations (GDPR). It is written for parish and town councils and parish meetings. It lists what you need to do and how and when to do it. This guide complements and should be read in conjunction with “*New Data Protection Laws – A GDPR Toolkit of local councils”* from the National Association of Local Councils (NALC), a copy of which was emailed to all member councils recently.

It is unlikely that any council will achieve 100% compliance by 25 May 2018 when GDPR comes into force, but completing steps 1 to 10 below will help demonstrate that your council is working towards compliance.

The **first part** of this guide walks you through the steps you need to take to create a Data Map. A Data Map sets out the data that the council holds, where it is and what happens to it. It’s like an asset register for data.

A sample Data Map in spreadsheet format has been created for you and included with this guide.

The **second part** of this guide lists the key documents and policies that your council needs to have in place. Model documents suitable for parish and town council and parish meetings have been created for you and are included with this guide. Your council will need to customise them and tailor them to your own needs and then formally adopt them.

We are working on the basis that every council will hold a meeting in May (the Annual Meeting) and that a resolution to approve the Data Map and adopt the documents can be on the agenda for that meeting. A sample agenda item is included on Page 5 of this guide.

Take your time working through this Quick Start Guide. There is nothing difficult or complex to do but you will need to be organised and thorough.

**Part One – Preparing the Data Map**

Open the sample Data Map on your computer (sample\_data\_map\_v1.xlsx). Familiarise yourself with the layout. Allocate no more than one to two hours to completing the tasks below.

1. Think about the information the council holds and where it is. The sample Data Map has been pre-populated to give you a start. Delete any rows that do not apply to your council and add rose for any types of information that are missing.

Complete columns A, B and C in the Data Map, this should include all the personal information the council has (contact details, photos, employee information, CCTV footage, financial information, employment information etc). Think about emails, paper files and computer documents.

1. Now you have listed the types of information your council holds, the next step is to think about how it is processed, stored and protected. Complete columns D, E and F in the Data Map.

**Top Tips**

* Insist on password protection of the clerk’s computer, councillors’ computers, mobile devices and external hard drives. Ensure anti-virus security packages are up to date.
* Keep parish council correspondence separate to other correspondence. The simplest way to do this is to assign a parish council email address to all councillors and to insist that if councillors use a shared computer, they have a login just for parish council business.
* Ensure all councillors complete the “GDPR Security Compliance Checklist” (a sample is included with this guide) and retain a copy for evidence.
* If you use cloud storage, where are the servers? Does the information go out of the European Economic Area? If it does, you will need to have assurances that the data is secure and document these assurances. Some companies (Microsoft, Google) are already preparing privacy statements which can be used to show compliance when using their systems.

1. Next, identify why you need the data and what the lawful basis for processing it is. Complete columns G and H. Every organisation must be able to show that they have a legal reason to use personal data. Parish councils will most likely be able to rely on “contract” (for employment related information and projects), “legal obligation” (employee payroll/pension requirements) and “public interest”. Using “consent” as a lawful basis is quite restricted for public authorities such as parish and town councils, so it is best to consider other lawful bases as described above.
2. Determine how long the council retains the personal data for. Complete Column I in the Data Map.

***A working version of your Data Map should be ready for adoption by your council at its May meeting. Remember it is a living document and should be reviewed regularly and added to or amended as appropriate. Your council is well on the way towards full GDPR compliance***.

**Part Two – Preparing your GDPR Documentation**

A suite of documents and policies are required in order to comply with GDPR. Samples of these documents are included with this guide. Familiarise yourself with them. They are intended to be simple to use. The documents must not be adopted by the council until they have been customised and tailored to the needs of the council. The key documents are:

* Privacy Notices (from the NALC Toolkit)
* Data Protection Policy
* Subject Access Request Procedure
* Data Breach Policy
* Records Retention Policy
* GDPR Security Compliance Checklist

1. Using the templates provided in **Appendix 4 of the NLAC Toolkit**, prepare your privacy notices. They must include the organisations name, how it will use the information, what lawful basis is used to process the data, how long the data will be kept and how a data subject can complain to the Information Commissioner’s Office (ICO) if they disagree with the way the data is handled. Adapt the templates so they are specific to your council and then they can be adopted by the council at the May meeting. They should then be published on the council’s website and issued whenever the council is seeking consent.
2. Prepare your Data Protection Policy, Subject Access Request Procedure, Data Breach Policy and Records Retention Policy (templates are included with this guide). Adapt the templates so they are specific to your council and then they can be adopted by the council at the May meeting.
3. Decide who the council’s Data Protection Officer (DPO) will be. To comply with GDPR your council must appoint a DPO will be the contact point for the ICO and will be able to advise the council of its GDPR obligations, monitor compliance, carry out/organise audits and raise awareness of GDPR and information governance issues. Lincolnshire CALC are still exploring a DPO service and what it will look like. This information will be available as soon as possible.
4. Determine if your council is registered with the ICO already (search the register of data controllers here: <https://ico.org.uik/about-the-ico/what-we-do/register-of-data-controllers/>). If your council is registered it does not have to pay the new Data Protection Fee until that registration has expired and you will receive notification from the ICO. If your council is not currently registered it will need to do so to comply with GDPR. The council should approve payment of the Data Protection Fee at its May meeting (£40 for most parish and town councils, with a £5 discount for paying by Direct Debit) and ensure that the council is registered on or soon after 25 May 2018.
5. Consider if your council uses third party data processors. For example, do you outsource payroll or CCTV? These are common examples of third party data processors. You must have a written contract in place with the processor. (Please see **item 29 in the NALC Toolkit** for more guidance).
6. Consider whether you need to put systems in place if you work with children and process their data (for instance the council may have consulted school children about new equipment in a play area or asked them to enter a competition). If you collect children’s data you must also have the consent of their parents or guardians and the consent must be written in simplified language to make sure the child understands what they are giving their consent to. Copies of all consents must be retained.

***Customised versions of all the key documents should be ready for adoption by your council at its May meeting. All documents should be reviewed regularly and added to or amended as appropriate.***

**Agenda Item for the May Meeting**

By law, all councils must meet in May for their Annual Meeting. This provides an excellent opportunity to include an agenda item specific to GDPR compliance. The recommended item is:

**X GDPR compliance**

a) To appoint [ ] as the council’s Data Protection Officer

b) To adopt the Data Map (enclosed)

c) To adopt the Data Protection Policy, Subject Access Request Procedure, Data Breach Policy and Records Retention Policy (enclosed)

d) To adopt the Privacy Notices (enclosed)

e) To receive completed Security Compliance Checklists from all councillors

f) To note that the council is already registered as a Data Controller with the ICO **or** (*delete as appropriate)* To resolve that the council registers with the ICO and pays the relevant Data Protection Fee

**Ongoing Compliance**

If the council plans to implement a new system (for example CCTV, new email system), the council must carry out a Data Protection Impact Assessment (DPIA). (Please refer to **page 25 and Appendix 6 of the NALC Toolkit** for detailed guidance).

Keep consent records up to date (review at least every 2 years) and renew consents every 5 years. Review the Data Map and amend if necessary. Review and update all GDPR documentation. This should be done at least annually.

**Glossary**

* **Data Map**  - a document that records the information collected when conducting an information audit of the council
* **Lawful Basis** (for processing data)
* **Contract –** use this basis if you must obtain data to enter into a contract, or comply with the terms of a contract
* **Legal Obligation** – use this basis if you are legally required to use the information, for instance to provide a pension, calculate tax and NI, or to perform a statutory power
* **Public Interest** – use this basis if you determine that processing the date is necessary to complete your tasks as a public authority
* **Consent** – must be freely given, and can easily be withdrawn which is why it should be used only if no other lawful basis is appropriate
* **Data Protection Officer (DPO)** – a person appointed by the council. See <https://goo.gl/1PYYF3> for information on the role of the DPO
* **Data Protection Fee** – the fee collected from all data controllers by the ICO. See <https://goo.glcNS5Nj> for more details
* **Cloud Storage**  - data is maintained, managed, backed up remotely and made available to users over the internet.

**This Quick Start Guide was produced by the Northants CALC. It is a deliberately concise guide and is not intended to provide all the information that councils will require to achieve full GDPR compliance. This guide should be read in conjunction with the NALC Toolkit and the information and guidance provided on the ICO website at** [**www.ico.org.uk**](http://www.ico.org.uk).