GDPR Proposals for consideration by Weeton Parish Council

Revision 1

14th January 2020

1. Foreword

The General Data Protection Regulation ("GDPR") took effect in the UK from 25 May 2018. Along with the Data Protection Act 2018, it replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by councils. Local councils and parish meetings must comply with its requirements, just like any other organisation.

The GDPR applies to all local councils and also to a parish meeting without a separate parish council because a local council and a parish meeting are public authorities. The GDPR states that organisations, including local councils and parish meetings will need to appoint a Data Protection Officer ("DPO") if they meet certain criteria. Local councils and parish meetings will not fall into the definition of a 'public authority' for the purposes of the Data Protection Act 2018. The rationale for this according to the debates in Parliament is that local councils and parish meetings will not normally be processing personal data 'on a large scale'. However larger local councils who do process personal data on a large scale may still have to appoint a DPO.

This document proposes actions needed by Weeton Parish Council to ensure compliance.

Given the limited scale and nature of the data we hold and use we do not anticipate any significant issues or difficulties. We intend to follow the guidance given by the National Association of Local Councils (NALC)

2. Proposals

The following Action Plan is proposed by NALC and it is proposed that Weeton Parish Council uses this as a means to ensuring compliance.

Action Plan

We should work through the steps in the Action Plan below. We should complete the process as quickly as possible in a manner that is appropriate for the scale of our data use. It was not expected that everyone would have completed this process by 25th May 2018.

1.	***Raise awareness –*** Councillors, staff, and volunteers, should be made aware that the law is changing. Ensure they undergo training, and that records are kept. They need to know enough to make good decisions about what you need to do to implement the GDPR. ***Decide who will be responsible for the council's compliance with data protection law –*** All councillors, staff, committees and sub- committees are expected to apply data protection legislation in their work. If you appoint a DPO, they should have access to full council and

	relevant staff, committees and sub-committees. Even if you do not appoint a DPO, it is helpful to designate one person responsible for co-ordinating compliance with the law and to coordinate efforts in the event of a subject access request or a data security breach.
2.	***Data Audit –*** If you do not know what personal data you hold and where it came from you will need to organise an audit to find out. This means reviewing personal data held in respect of staff and volunteers, people using council facilities or services, councillors, contractors, residents, and more. You should document your findings because you must keep records of your processing activities. You should also record if you share data with any third parties.
3.	***Identify and document your 'lawful basis' for processing data –*** To legally process data under the GDPR you must have a 'lawful basis' to do so. For example it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and different lawful basis give different rights to individuals.
4.	***Check your processes meet individuals' new rights –*** The GDPR will give people more rights over their data. For example, the GDPR gives individuals the right to have personal data deleted. Would you be able to find the data and who would be responsible for making sure that happened? Ensure you have the systems in place to be able to deliver the 8 rights. ***Know how you will deal with 'subject access requests' –*** Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a 'subject access request' or "SAR". You need to be able to identify a SAR, find all the relevant data and comply within one month of receipt of the request. Under the GDPR the time limit for responding to SARs is reduced from 40 days to one calendar month and the £10 fee is abolished.
5.	***Review how you get consent to use personal data –*** If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under the GDPR consent must be freely given, specific and easily withdrawn. You can't rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in.
6.	***Update your Policies & Notices –*** Have clear, practical policies and procedures for staff to follow, and monitor their operation. ***Privacy Notices -*** You must tell people in a concise, easy to understand way how you use their data. You may well already have privacy notices but they will all need to be updated. Under the GDPR privacy notices must give additional information such as how long you will keep data for and what lawful basis you have to process data. ***Data Retention & Disposal –*** Ensure you update your data retention policy and inform all data subjects how long you will retain data. When disposing of records and equipment, make sure personal data cannot be retrieved from them. ***Websites –*** Control access to any restricted area. Make sure you are allowed to publish personal data (including images) on website/social media. ***Data sharing –*** Be sure you are allowed to share personal data with others and make sure it is kept secure when shared. ***CCTV –*** Inform people what it is used for and review retention periods. Ensure you have the correct signage on display and a suitable policy in place.

	Training – Train staff on the basics of personal data security, where the law and good practice need to be considered, and know where to turn for advice.
7.	***Build in extra protection for children*** – The GDPR says children under 16 cannot give consent, however the DPA 2018 has amended this in the UK to 13. If a child is under 13 years of age you will have to obtain consent from a parent or guardian. You will need to be able to verify that person giving consent on behalf of a child is allowed to do so. Privacy notices should to be written in language that children can understand.
8.	***Update your contracts to deal with processing by others –*** Recognise when others are processing personal data for the council and make sure they do it securely. You will need to ensure your contracts are updated to include the GDPR required clauses and put in place an audit programme to supervise them. Consider also how you select suppliers. There must be a written contract which imposes these obligations on processors:

1. Follow instructions of the controller. 2. Ensure their personnel are under a duty of confidence. 3. Keep the personal data secure. 4. Allow the controller to consent to sub-contractors. 5. Flow down obligations to sub-contractors (but remain responsible for actions of the sub-contractor(s). 6. Assist the controller when individuals exercise their rights to access, rectify, erase or object to processing of data.	7. Assist the controller with privacy impact assessments. 8. Assist the controller with security and data breach obligations and notify the controller of any personal data breach. 9. Return or delete data at the end of the agreement (but can keep a copy). 10. Demonstrate compliance with these obligations and submit to audits. 11. Inform the controller if their instructions would breach the law.

9.	***Personal Data Breaches - Get ready to detect report and investigate these -*** A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. You will need to have the right procedures in place to detect, investigate and report a breach. The GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned. You need to be able to demonstrate that you have appropriate security, technical and organisational measures in place to protect against a breach. If there is no risk of harm to an individual (for example because some low risk data has been inadvertently released or made public such as an email address) then this type of breach would not need to be reported. Unauthorised access to data that could be used to steal someone's identity such as their banking data must be reported. ▪ The DPO or designated data protection compliance officer should be involved after the council becomes aware of a data breach. ▪ Councillors, staff, contractors and the council's data processors should be briefed on personal data breach avoidance, and on what to do in the event that a breach occurs. ▪ Examples of personal data breaches and steps to avoid them include: – Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking 'send'.

	– The wrong people being copied in to emails and attachments. – Use BCC (Blind Carbon Copy) where necessary. – Lost memory sticks which contain unencrypted personal data – The council should put protocols in place for memory stick usage – Malware (IT) attach – ensure up to date anti-virus software is in place. – Equipment theft – check security provisions. – Loss of personal data which is unencrypted
10.	***Build data protection into your new projects*** - Privacy by design means building data protection into all your new projects and services. It has always been good practice, but the GDPR makes privacy by design an express legal requirement. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale. Clarify who will be responsible for carrying out impact assessments, when you will use them and how to record them.
11.	***Consider if you need to appoint a Data Protection Officer.***

3. Timescale

I would propose that some aspects are addressed immediately such as Privacy Notices using the NALC standard format and these should be uploaded to the Councils website.

Other items should be addressed progressively with an aim to be compliant as soon as possible.

Paul Jagger

14th January 2020