New Data Protection Laws (GDPR) and how this affects us as Huntington Parish Council

AT A GLANCE AND EASY-TO READ

March 2018

This is an 'at a glance' summary of the new Data Protection Laws that are coming into place on the 25th May 2018 and how it affects us as Huntington Parish Council.

Please Note: This is NOT completely comprehensive and there are other elements to this law that will be required to be implemented at a later date. However, I have prioritised that which needs immediate action or needs to be in place as priority.

The GOOD NEWS

- NALC acknowledge that Parish Councils have to process this new legislation and implement it, with not long to do it. They state:

"You should work the steps in your action plan [using the template they provide]. You may not complete all of the steps by 25th May 2018 when the GDPR comes into force but you should have a plan in place to complete the step

- Chalc are planning to run training on this which will highlight any gaps we may have and how to solve them

- We are already registered with the ICO and have been for some years (thanks to your previous Clerk). This is a head start on many Parish Councils who have never registered. By being registered, it has meant that we are compliant with the Data Protection Act 1998, which requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence. Under the new regulations, we do NOT have to register with the ICO BUT we will have to legally pay a Data Protection Fee. By being on their database already, it means we will automatically be notified about this.

There are more than half a million registered data controllers. ICO publish the name and address of these data controllers, as well as a description of the kind of processing they do.

WHY DO WE NEED TO DO THIS?

The General Data Protection Regulation ("GDPR") will take effect in the UK from 25 May 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.

WHAT DO WE HAVE TO DO?

I have devised an action plan to highlight the PRIORITIES that we, as Huntington Parish Council, have to do. ***Below the action plan is further detail of each element and the legal obligations surrounding it.***

Action	By Whom	By When
1. Carry out an Audit of data kept by Huntington Parish Council	Clerk	By 25th May 2018
2. Create Privacy Notices for a. Residents/General public b. Councillors/Staff *Please note: NALC provide templates which I include in this report BUT they will need editing to be more applicable with our Parish Council*	Clerk	By 25th May 2018
3. Create Consent forms for our Resident Distribution list (who receive agendas, works programme and links to docs each month). *Please note: NALC provide templates which I include in this report BUT they will need editing to be more applicable with our Parish Council*	Clerk	By 25th May 2018
4. Create a policy for 'Subject Access Requests'	Clerk	By 25th May 2018 or as soon after
5. Create a Policy for Data Retention, Data Disposal and what our procedure is if a data breech occurs.	Clerk	By 25th May 2018 or as soon after
6. Appoint a Data Protection Officer who will oversee our Data Protection policies and advise *Please Note: This point is still being disputed by NALC in govt. They argue that this is an extra cost burden for PC's but some argue that a Clerk could do this role. HOWEVER, a DPO is meant to oversee the Data Protection Controllers role (most often the Clerk) and make sure they are doing it properly – I wouldn't be able to audit myself! Chalc will give an update when resolved*	Clerk and selected Councillors?	By 25th May 2018 or as soon after
All of the above will need to be approved by Full Council before adopting it as policy.		

WHAT WILL THE AUDIT OF DATA TELL US?

It will highlight any data that we process/store that we may not have previously thought of. This can then ensure that this data will be stored/process in compliance with the new Data Regulations

For example: If we as a council process personal data but have no access controls in place restricting who can see or use the data, that is a security risk which needs to be fixed. Without carrying out an audit, we may not know what risks we currently have with our data.

The 'Personal Data' section provides a good and very real example of this, it suddenly occurred to me that we hold data of business bank account details whenever they send us an invoice. 'You', as a Parish Council, also hold my bank account details to pay the Clerk's Salary. This all needs specification in how we as a Parish Council **PROTECT** those details.

Template for the AUDIT – page 28 - 30 of the GDPR toolkit

WHAT DO RESIDENTS NEED TO CONSENT TO?

From 25th May, under the new GDPR laws, residents **must** give consent for us to hold their email on account and send them documents such as newsletters, monthly agendas and works programmes. This is an OPT-IN process, not opt-out which means they HAVE TO fill in a consent form if they want to stay on the distribution list. **(I fear this may result in us losing a significant number of our 90+ residents who we email as they won't fill in the form!)**

NALC state: "*This consent is for general terms such as holding residents email to distribute them an agenda. It is NOT for specific issues such as complaints"*

Passing emails to CW&C is different and would need a different type of consent.

Eg: If a resident contacts me complaining about a hedge that had overgrown onto a pavement. I would then need express permission to pass that email onto you as Cllrs and onto CW&C Streetscene. Therefore, I would have to write back to them, acknowledging the complaint and asking if I can pass their details/email on.

TEMPLATE OF A CONSENT FORM FOR RESIDENTS/GENERAL PUBLIC – page 31 of the GDPR toolkit

(

DOES THAT MEAN THAT I AS A COUNCILLOR WILL NEED TO GIVE THE CLERK CONSENT TO PASS MY EMAIL ON/GIVE OUT MY EMAIL ADDRESS TO RESIDENTS?

No! Your email address HAS to be freely made available such as on notice boards and on the website (This does NOT apply to your personal email, ONLY your Huntington Parish Council email). This also applies to the Clerk email address, 'office' address and 'office' phone number (which is also my home phone number and address in this situation)

NALC states "A councillor does not have a free choice to withhold their consent to the processing of their personal data in connection with the role

they are performing in the council. This means that 'consent' is not an appropriate legal basis to process personal data for staff or councillors"

Basically, this means that when you sign the declaration to be a Councillor, you agree that your regs of interest including the information held on it PLUS your Councillor Email address will be made available to the public.

It also means that any documents, produced by the Parish Council which features your name on it, can be still made public (as long as it does not contain sensitive information such as appraisals, disciplinary matters, salary details etc.). It also means that **FOI requests made**, which may include your emails sent to the Clerk address/from your publicised Councillor email address can STILL be included in the FOI information that I have to provide.

NALC states: Gaining Consent applies in most cases to local residents but not to personal data which is processed in connection with a person's role in the council. For example, staff and councillors cannot give valid consent because consent has to be "freely given". A staff member or councillor cannot be said to be freely giving their consent, because the balance of power between them and the council is not equal. A staff member or councillor cannot 'choose' to withhold their consent or to exercise their right to withdraw it. If a staff member were to withdraw consent, this would put the council in an impossible situation, as it would be obliged to continue to process the personal data whilst the individual carries out their role.

WHY DO WE NEED TO PRODUCE PRIVACY NOTICES?

In order to know what residents are consenting to and how we are going to be using their data if we do keep it on file, we need to produce Privacy notices, outlining how we use personal data.

WHY DO COUNCILLORS/STAFF NEED DIFFERENT PRIVACY NOTICES TO RESIDENTS?

For the reasons stated above within the consent information. Your privacy rights are different to that of residents.

Templates of the following (which we have to edit and adopt) are available on the GDPR Toolkit:

- *Sample Privacy Notice for Residents/General Public* – ***Page 32-35***
- *Sample Privacy Notice for Councillors/Staff of the Parish Council* – ***page 36-41***

WHAT ARE 'SUBJECT ACCESS REQUESTS' AND HOW DOES THAT AFFECT US AS HUNTINGTON PARISH COUNCIL?

NALC states: ***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.

We will need to produce a policy which informs the public of our approach to SARS and what they should expect if they implement a SAR

PLEASE NOTE: This is different to a 'Freedom of Information' request. A FOI can request documents that we as a PC hold. A SAR is a request to see what data we hold on the person who requested.

Templates of the following are available on the GDPR Toolkit

- SAR Process checklist for Parish Councils (in the case that we receive one) – **pages 48-49**
- Sample 'Subject Access Request' policy that we could edit and adopt **– page 49-50**
- Sample Response letters to a Subject Access Request– **page 50 - 51**
    (a) Agreeing to the request and providing the information
    (b) Agreeing to the request in part but withholding some information and the reasons why we have to withhold it
    (c) Refusal to accept the request and the grounds for doing so

WHY IS IT IMPORTANT TO CREATE A DATA RETENTION AND DISPOSAL POLICY?

The new regulations state that we have to have consent to hold personal data on file, which includes email addresses and names. This means that any CURRENT emails from residents that we have on file must have consent, which we obviously don't have at present.

NALC state: ***A Data Controller [most often the Clerk] must delete personal data unless there is a legal obligation to retain the personal data. Data deletion processes will need to be introduced so that data is not retained indefinitely. It's likely a "data cleansing" exercise will need to be carried out prior to 25th May 2018 so that the council is not storing data it no longer requires or has a need to retain. When disposing of records and equipment, we must also make sure personal data cannot be retrieved from them.***

CHALC advice: Delete everything once it has been dealt with.

Therefore, we must ensure that we have a data retention policy and inform all data subjects how long you will retain data. We must also include details of what we will do if a security breech has occurred.

WHAT COUNTS AS A SECURITY BREACH?

Nalc state: *A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal*

data'. For example: Unauthorised access to data that could be used to steal someone's identity such as their banking data must be reported.

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.

For example: If I send out the Agenda to the 91 residents on our distribution list and accidentally forget to do a Blind copy (BCC) on it, it means that I have just exposed 91 email addresses to the other people in the list. This would be bad practice and I should send an apology to all residents involved but would not need to be reported to the ICO as it would not cause harm to the individual

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
- Ensure up to date anti-virus software is in place.
- Equipment theft – check security provisions.
- Loss of personal data which is unencrypted

WHY DO WE NEED A DATA PROTECTION OFFICER AND WHAT DO THEY DO?

The Clerk is, in most Parish Council cases, the Data Protection CONTROLLER. It is the controller or the processor, NOT the officer, who is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'.

The GDPR sets out in detail the minimum responsibilities of the Data Protection Officer ("DPO") role. GDPR specifies that DPOs "should assist the controller or the processor to monitor internal compliance with this Regulation"

For details on the Responsibilities of the DPO – Page 42 – 43 of the GDPR handbook