AGENDA ITEM No 6

BRIEFING ON MEMBER OBLIGATIONS UNDER GDPR

NOTE - the following is copy guidance issued for elected Members of a principal Council and reproduced with its consent. Although some of the organisational arrangements are different to those of Tavistock the principles are transferrable and the practices applicable.

Organisational issues can be explored at https://ico.org.uk/for-organisations/local-government/local-gov-gdpr-faqs/

General Data Protection Regulation – an Overview

The law relating to data protection is changing as from 25th May 2018 and the Data Protection Act 1998, that has been in place since before the use of the internet, emails and cloud storage services, will be repealed on or before this date which is when the General Data Protection Regulation (GDPR) comes into UK Law.

The GDPR will enhance the rights of data subjects and give them greater access to their data and more control over what happens to their data. It also gives an individual data subject the right to ask us to stop processing their data if we are not processing it for a statutory reason (i/e Council Tax) and gives rights for a data subject to be 'forgotten' and have data removed from the system, or for it to be rectified if it is shown when we hold is inaccurate.

GDPR allows for increased financial penalties to be imposed on any organisation that breaches a data subjects rights or does not comply with the accountability principle – which basically means that the Council needs to ensure that it has the right measures in place to protect the data from loss, unauthorised access to is etc and to ensure the rights of data subjects as set out in the legislation are protected.

Also, under GDPR, data that is stored will be considered to be data that is being processed and is subject to the same rules as all other data you hold.

What is personal data under GDPR?

We hold data in many different formats, paper and electronic as well as audio and visual recording and GDPR applies to any data from which a living subject can be identified.

This includes but is not limited to:

- an identifier, eg a name, email address, phone number
- personal identification numbers, eg bank account, national insurance number;
- factors specific to an individual's physical, physiological, genetic, biometric mental, economic, cultural or social identity. This would include anything about a disability or a finger print.

New kinds of identifying information which GDPR includes in the definition of personal data are:

- location data - data that has any kind of geographic position attached to it, eg data collected by wireless networks, swipe cards and smart mobile devices that provide location tracking
- online identifiers, eg mobile device IDs, browser cookies, IP addresses

Special Categories of Data are those which are particularly sensitive regarding, race, ethnicity, political opinion, genetic or health related data and sexual orientation.

The broadening in the definition of personal data is important because it reflects changes that have occurred over the past few years in technology and the way that organisations collect data about individuals.

As a Data Controller registered with the Information Commissioner's Office you will need to comply with the new legislation when it comes in force.

You should already be keeping personal data secure and only using your official email address to respond to Council matters. You are already aware to be careful with whom you share personal data and to keep information for no longer than you need to.

The new Act will place a personal duty on you as an individual controller to keep certain records as it is your duty to show that you are complying with the law. It is also designed to give data subjects (your constituents) greater rights to control, access and remove the data you hold about them.

New requirements:

- If you collect data for a local project, such as via a petition you may need to underpin this with a Privacy Notice;
- You need to delete 'old' data you no longer need (referred to in GDPR as data minimisation); and
- You are required to report any data breaches to the ICO within 72 hours.

Record Keeping:

To comply with the Act you must keep certain records if your processing is more than occasional (we would suggest this is for complex complaints and a large case work matters) or you are processing *'special categories of data'* e.g. anything concerning race, religion, health, sexual orientation etc. It is possible that you will have health data concerning your constituents and you should record (perhaps in a word document):

The details that should be recorded are:

- The name and contact details of the Data Controller – yourself;
- The purpose of your processing and legal basis for it e.g. to investigate complaints/casework;
- The categories of data you hold, e.g name and address, email, medical information for constituents and complainants;
- Anyone you share the data with e.g. other Councillors/Council Officers/other services;
- How long you will keep the data for e.g. 6 months after the case is closed;

- What security you have in place to protect it e.g. password protection, only using secure CC provided email address, storing documents on a CC device or storing documents locking in a cupboard etc.

NOTE: As you are registered as a Data Controller in your own right The Information Commissioner can ask to see this record to ensure your compliance.

Privacy Notices

If you collect data locally, say to obtain views for or against a local project, you are required to give a Privacy Notice to the person you collect personal data from at the time you collect it.

This could be a standard paragraph at the end of an email when you acknowledge receipt of a complaint or you can give it verbally if you take a telephone call in which case you should record that you have given it verbally.

You should not use personal data other than for the purpose which you stated when you collected it, therefore if you collect the data about a local road improvement scheme, you cannot then use this for a local supermarket scheme or keep the contact details and use them for direct marketing or political purposes.

If you wish to use the data for another purpose then you should return to the person and seek their consent for this additional processing. If you are collecting special categories of data then the person should give you explicit consent to process this data; we suggest this means you obtain their signature and you should keep a record that they have given consent.

A Privacy Notice should include:

- That you are the Data Controller and your contact details;
- The purpose of processing and legal basis for doing so (to assist with their complaint);
- Who you will share it with e.g. other Councillors/Council Officers/ any other agencies;
- The retention period i.e. how long you will keep it for e.g. for 6 months after their complaint has been finalised;
- That they can withdraw their consent to you processing their data by contacting you and asking you to stop doing so;
- That they can access a copy of the information you hold, ask for it to be corrected if it is wrong or for it to be deleted;
- To contact you if they have a complaint about how their data is handled and if it is not resolved to contact the ICO.

Rights

As stated in the Privacy Notice you must comply with certain rights which the data subjects have. This includes allowing them to access all the data you hold on them, this is usually by way of a copy of emails or letters. You have one month to comply with a request for personal data which is called 'subject access request'.

You must remember NOT to supply the requestor with anyone else's personal data as they are only entitled to access their own.

NOTE: a subject access request is made under different provisions from a request for information made under the Freedom of information Act.

Any data subject can also ask for their data to be corrected, moved, restricted or erased in certain circumstances. Again, we can assist if you receive a request to do this.

Security

You should ensure the security of the personal data that you hold by only using your official email address and being careful if you work in public areas so that you are not overlooked. You should not leave documents or unlocked computers/ipads on whilst you are out of the room and should ensure that you have a password to access the necessary files. You should ensure the device that you use is stored securely when not in use. When emailing you should put the minimum amount of personal data necessary in order to make sense and avoid references to other identifiable people where possible.

If you use the tablets and email addresses provided these have all be checked in order to ensure that they are secure and, if a breach occurs because unauthorised access is gained to them the liability rests with the Council, but this is not the case if you use your own devices.

'old' data

You should not be routinely keeping all the cases that you have assisted with in the past. You must decide how long after you have closed a case to keep it for and after this period you should securely delete any files containing that data.

We would suggest that between 12 - 18 months is an appropriate length of time to retain case work files for.

Reporting a personal data breach

The new Act will set a time limit of 72 hours of reporting a personal data breach to the ICO if it will result in a risk to the data subject. It is expected that their online breach reporting system will continue.

The Local Government Association have set out that they will be publishing further advice and hopefully an e-learning module specifically for members in early 2018 and there will be in house face to face training offered to members in he late spring of 2018.

Whilst the above may appear onerous the Council is already fully compliant with the requirements of the Data Protection Act and we have such additional requirements, such as breach reporting, already in place. However, the Information Governance Team can offer advice and assistance on any matters relating to GDPR and discuss with you any concerns you may have about the introduction of the new regime.

Example of a Privacy Notice:

Application for a Temporary Event Notice – Licensing Act 2003.

Data Protection Notice
East Lindsey District Council is a Data Controller and can be contacted at: Tedder Hall, Manby Park, Louth, Lincolnshire, LN11 8UP. Tel 01507 601111. The Data Protection Officer is (*awaiting confirmation)* and can be contacted at the same address.

We are collecting your personal data in order to process your application under Licensing Legislation as we are the Licensing Authority.
Your data will not be shared with third parties but may be used for Council purposes, in order to prevent or detect crime, to protect public funds or where we are required or permitted to share data under other legislation.
Your data will be kept for 6 years in line with our retention policy.
You have the right to access your data and to rectify mistakes, erase, restrict, object or move your data in certain circumstances. Please contact the Data Protection Officer for further information or go to our website where your rights are explained in more detail. If you would like to receive an explanation of your rights in paper format please contact the Data Protection Officer.
Any complaints regarding your data should be addressed to the Data Protection Officer in the first instance. If the matter is not resolved you can contact the Information Commissioner's Office at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Tel: 0303 123 1113

If you do not provide the information required on the form then we will not be able to process your application for a licence.
For further information on our Data Protection Policies please go to our website.