**HANDOUT SIX**

# Data Protection

**Sources of information** – Information Commissioners Office (ICO) website; National Association of Local Councils (NALC) Legal Topic Note (LTN) 38: Data protection (Dec 2018) and LTN 40: Documents and records. (November 2016), NALC Data Protection Toolkit.

## Data protection legislation

Primary legislation is an Act or Statutes of Parliament (in England) or the Senedd (in Wales), the Data Protection Act 2018
Secondary legislation or supplementary regulations are those granted by additional law making powers delegated to another branch of government (in England) or Welsh ministers by an Act or Statute, the UK General Data Protection Regulation 2018 (UK GDPR).

## What data are we especially concerned about?

**Personal Data**. Personal data is information relating to a living, identified or identifiable individual by name or address. If it is possible to identify a living individual from the information that you're processing, it is likely to be personal data. Before collecting or keeping personal data, councils should consider why the information is being held and on what legal basis and tailor their personal data collection accordingly. To be transparent, open and accountable, Councils should clearly express what they are using the personal data for. Where collecting personal data is based on consent, the Council must be able to evidence that consent and it must be by an 'opt in' method. Further consent should be obtained to use the data for anything except what it was collected for originally. Consent to hold certain personal data for staff, volunteers and councillors must be freely given (by law) to allow them to perform their role. The individual should however, be aware of what information the Council holds for them and it should not be shared without their consent. Individuals have certain rights associated with data:-

The right to be informed
Right of access
Right to rectification
Right to erasure
Right to restrict processing
Right to data portability
Right to object
Rights in relation to automated decision making and profiling.

Under the Data protection Act 2018, Section 7, a parish council in England or community council in Wales does not have to appoint a **Data Protection Officer** (DPO) to advise on data protection and look into breaches of the code. However, it is helpful for a council to have a process in place for handling any queries relating to data protection.

**Data controllers** determine the purposes and means of processing data and they must pay a data protection fee to the ICO unless they are exempt. Data Controllers must report certain types of data breaches to the ICO without 'undue delay' (within 72 hours of being aware of the breach where possible). The Council as a corporate body is the Data Controller rather than any individuals. If you work for the Council then you will be an employee of the data controller. Councillors are encouraged to hold as little personal data as possible and use a recognisable council e-mail address.

**Data processers** follow the instructions of someone else but have legal obligations to maintain records of personal data and processing activities.

## What are the key principles of data protection?

The ICO identifies there are 7 principles which should be at the heart of a Council's approach to processing personal data:-

1. Lawfulness, fairness and transparency
2. Purpose limitation – only collect data with an end purpose in mind.
3. Data minimalization - only collect what you need to.
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability.

## Core documents

The NALC Toolkits offer guidance on the range of forms which may be required to suit your Council's activities but a selection of core documents that may be used are as follows:-

**Personal Data Protection Policy** - sets out how your organisation protects personal data.

**Data Privacy Notice** – public statement of how your organisation applies and complies with the GDPR's data processing principles.

**Data Retention Policy**– How data is organised so that it can be easily accessed at a later date, how long information will be retained and how information will be disposed of when it is no longer required.

**Data Privacy Impact Assessments (DPIA**) – these are mandatory in certain situations and contain a description and purpose of the data processing and identify risks to personal data along with ways of mitigating the risks. The mandatory situation could be, for example, when installing new technology or when activities which use automated processing to evaluate analyse or predict behaviour are being used (Survey Monkey or questionnaires).

These link to an overall **Data Protection Impact Assessment Register** – an audit of where the organisation gets data, where it's held and how it's processed and any risks.

**Subject Access Request Policy/ Procedure** – to enable an organisation to respond if there is a request about personal information. The time limit to comply with a Subject Access Request is one calendar month.

**Data Breach Response and Notification Procedure and Register** - some breaches should be notified to the ICO and the facts surrounding the breach, the effects and any remedial action taken should be noted. If there has been a personal data breach which is likely to result in a "high risk to the rights and freedoms of an individual" the individual needs to be informed.

The following policies / forms may be used in some councils.

**Data Subject Consent Form** – to obtain permission from data subjects to allow personal data to be processed for a specific purpose. There must be a written contract in place with another organisation if they process information on your behalf.

**CCTV Policy and code of practice** – assesses the impact of installing CCTV, including mitigation measures.

### What processes does your council have in place to put the legislation into practice?

1. Data protection training for staff and members.
2. The Council registers the information that it holds with the ICO and pays an annual "data protection fee".
3. Data Protection Impact Assessment Register is reviewed and updated annually.
4. A clear process for handling data queries and a Data Privacy notice explaining how the organisation handles personal data is available on the organisation's website.
5. Policies are reviewed regularly (annually or biannually) or following a change in data processing or guidance.
6. Data privacy impact assessments are carried out on any new activity.
7. Personal data is kept securely in locked cabinets or on password protected computers.
8. Councillors have identifiable council specific e-mail addresses to separate their personal e-mails from those sent in relation to council work.
9. Additional protection for children under 13 so that consent is obtained from a parent or guardian.

Version 4 1.12.2021 PW