General Data Protection Regulation (GDPR) Guidance

"The primary objectives of the GDPR are to give citizens and residents back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation was adopted on 27 April 2016 and applies from **25 May 2018** after a two-year transition period.

The GDPR builds on Data Protection Act 1998 principles already in place and reflects the Caldicott Principles.

Article 5 of the GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Article 5(2) evidencing compliance

The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

In order to comply the Council must:

- have appropriate technical and organisational measures that ensure and demonstrate that it complies. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- have relevant documentation on processing activities.
- appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - Data minimisation;
    - Pseudonymisation;
    - Transparency;
    - Allowing individuals to monitor processing; and
    - Creating and improving security features on an ongoing basis.
    - Use data protection impact assessments where appropriate.
- Adhere to approved codes of conduct and/or certification schemes e.g. ISO 27001 or NHS IG Toolkit Level Two

Records of processing activities (documentation)

As well as obligation to provide comprehensive, clear and transparent privacy policies the Council must maintain additional internal records of your processing activities. There are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

Additional Internal records:

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

The Council may be required to make these records available to the relevant supervisory authority for purposes of an investigation

Advice from the Information Commissioners Office (ICO)

What's new in GDPR: (click on links below)

- Introduction
- Principles
- Key areas to consider
- Individuals' rights
    1. The right to be informed
    2. The right of access
    3. The right to rectification
    4. The right to erasure
    5. The right to restrict processing
    6. The right to data portability
    7. The right to object
    8. Rights related to automated decision making and profiling
- Accountability and governance
- Breach notification
- Transfer of data
- National derogations

Changes to Consent Definition

One aspect of the GDPR which will require careful consideration, prior to its implementation, concerns changes to the way consent is obtained for processing personal data. The GDPR makes the definition for consent clearer than current legislation and directives:

DP Directive definition:	GDPR Definition:
"*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*	"*any freely given, specific, informed and **unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her"*

(Information Commissioner's Office, 2017)

Whilst key elements of the consent definition remain the GDPR has enhanced the definition. This definition can be considered further:

- *freely given* – consent must not be conditional on a service;
- *specific* – one consent for one issue, should not lump issues together;
- *informed* – the data subject should be informed on its use – how it will be used, by whom and how they can withdraw their consent;
- *unambiguous* – must be simple to understand and specific;

- *clear affirmative action* – an individual must agree in some tangible way that a data controller can record and keep their personal data so that the data controller can prove it was given and what they were told, when and how the data subject gave their consent

This definition, however, is only the starting point for the new GDPR standard of consent. There are several new provisions on consent within the GDPR which contain more detailed requirements:

- provisions on keeping records of consent,
- clarity and prominence of consent requests,
- the right to withdraw consent; and
- avoiding making consent a condition of a contract.

The GDPR, therefore, is putting a much greater emphasis on individuals having clear granular choices upfront and ongoing control over their consent.

Further information can be found in the ICO document Preparing for GDPR – 12 Steps