General Data Protection Regulation	**15 May 2018**
Corporate Policy and Resources Committee	**FOR INFORMATION**

Linkage to Council Strategy (2015-19)	
Strategic Theme	Leader and Champion
Outcome	Provide civic leadership to our citizens
Lead Officer	Head of Policy and Community Planning
Cost: (If applicable)	

1.0 General Data Protection Regulation – A New Privacy Framework

1.1 The General Data Protection Regulation (GDPR) is an EU Regulation which will apply across the European Union, including the United Kingdom, from 25 May 2018. As an EU Regulation it does not need to be transposed into UK law.

1.2 Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act 1998. However, it was recognised that much has changed since 1998 and the GDPR aims to try and address the wide range of new impacts on how your personal data is gathered, dealt with and protected by public and private sector organisations.

1.3 The new legislation creates an obligation for organisations such as the Council to understand the risks that they create for others in relation to their personal data, and to put in place measures to try and mitigate those risks.

2.0 What is Personal Data?

2.1 The GDPR has expanded the definition of "personal data" to mean:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be ***identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.***

2.2 The GDPR also specifies “Special Categories” of personal data which includes information on an individual’s Health, Religion, Race, Sexuality, Trade Union membership, and Genetic and Biometric information.

2.3 In addition the GDPR also requires personal data relating to children to be given particular protection with regard to areas such as marketing and consent for online services.

3.0 New Obligations on Council

3.1 The GDPR places greater emphasis on accountability and the documentation that a data controller such as the Council must keep to demonstrate their accountability. Compliance with the GDPR had required require Council to review its approach to governance and how we manage data protection as a corporate issue.

3.2 The Council is putting in place a framework that mainstreams privacy considerations throughout all that we do (“Privacy by Design”) and has put in place comprehensive but proportionate governance measures such as:

- reviewing existing data protection policies;
- the undertaking of an Information Audit;
- providing appropriate training for staff;
- providing privacy notices where appropriate;
- putting in place data sharing agreements where appropriate; and
- undertake Data Protection Impact Assessments on any new systems or processes that we introduce.

3.3 The Council must be very clear on the lawful grounds it is using in order to gather and process personal data and these include our legal obligations, contract, in the public interest or via ‘consent’.

3.4 Individuals who provide the Council with personal information will have stronger rights to be informed about how the Council is using their personal information and they’ll have the right to request that their personal information be deleted or removed if there’s no compelling reason for an organisation to carry on processing it.

3.5 The right of an individual to access information held on them by Council remains but there will be a reduction in the time allowed for the Council to process these Subject Access Requests. The requirements for consent to allow the collection of personal information have also been strengthened.

3.6 The Council will have to report any major data breaches posing a risk to individual’s rights and freedoms, and have a detrimental effect on those individuals, to the Information Commissioners Office (ICO). Data breaches now have to be reported to the ICO within 72 hours. A data breach can result

from the loss, destruction or alteration of personal data or through unauthorised disclosure of or access to personal data.

4.0 GDPR Principles:

4.1 The Principles contained in the GDPR are similar to the Data Protection Act 1998 but there are now six principles with a new principle included relating to demonstrating compliance:

- Personal data processed lawfully, fairly and in a transparent manner
- Accurate and, where necessary, kept up to date, and rectified without delay
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Collected for specific, explicit and legitimate purposes
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security
- The controller shall be responsible for, and be able to demonstrate, compliance