Appendix 2

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now:

1 Awareness.

The Council must make sure that key decision makers and key people in the Council are aware that the law is changing to the GDPR and that they are aware the impact this will have.

2 Information we hold.

The Council must document what personal/sensitive data it holds, where it came from and who it is shared with. An Information audit must be undertaken across the Council.

3 Communicating privacy information.

The Council must review all current Privacy Notices across the Council and put a plan in place for making any changes in time for GDPR implementation.

4 Individual's rights.

A review of all the Council's polices, and procedures will need to be undertaken to ensure the Council can deliver the new individual's rights including how the Council deletes data or provides data electronically and in a commonly used format. There are significant enhancements to the rights currently enjoyed under the DPA.

- **Right to rectification**. The Council must review its process for handling requests to rectify personal data to ensure compliance.

- **Right to erasure/right to be forgotten.** An individual has the right to be forgotten which enables them to request deletion or removal of personal data where there is no compelling reason to retain. The Council must assess how this can be achieved and technical arrangements must be put into place to respond to requests.

- **Right to restrict processing.** The process to handle requests to ask the Council to stop processing their personal data must be reviewed to ensure right can be actioned.

- **Right to data portability**. Data held in systems must be reviewed to ensure it can be transferred in a machine-readable format e.g. CVS file.

- **Right to object**. The process for enabling an Individual to exercise their right to object to process must be reviewed and included in Privacy Notices.

- **Right regarding automated decision making and profiling.** The Council will need to review any processing of personal data that results in an automated decision (if any) to ensure that an individual is able to request human intervention.

5 Subject access requests.

We must update our procedures for dealing with subject access requests and how we will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data.

The lawful basis for processing changes under GDPR. We must identify the lawful basis upon which we process personal data under the new grounds in GDPR. We must then document this and update our privacy notices to explain it.

7 Consent.

GDPR sets a high standard for consent. We must review how we seek, record and manage consent and whether we need to make any changes. We will also need to refresh existing consents now if they do not meet the new GDPR standard.

8 Children.

We need to consider whether we need to put in place systems to verify individual's ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches.

We must review our processes and procedures for detecting, reporting and investigating personal data breaches including the new duty to report to the ICO. We must assess the types of data and identify where the requirement to notify the ICO or affected individuals applies. The penalties are significant going forward increasing from the current maximum of £500,000 to £20m.

10 Data Protection by Design and Data Protection Impact Assessments.

GDPR requires Data Protection Impact assessments to be undertaken in specific circumstances. They are a tool to help identify the most effective way to comply with data protection obligations and meet the privacy requirements of individuals. What must be in an impact assessment is prescribed. Consultation is required with the ICO in some cases. We must carry out a review of our current process together with the creation of a technical measure to ensure the process is integrated into processing activities by design. The Crown Commercial Service has issued guidance for central government on how to integrate requirements into both current and new contract/procurement processes which the Council should review and follow.

11 Data Protection Officer.

There is a responsibility to appoint a DPO based upon expert knowledge of data protection law and practices and ability to fulfil the tasks in Article 39 of the GDPR. The DPO shall report directly to the highest management level.

12 International.

If the Council carries out cross border processing the lead data protection supervisory authority should be determined.

END