Appendix 1 – Key Changes

1. Key Principles

1.1 The GDPR updates and enhances controls on the processing of personal data. This includes any information relating to an identified or identifiable natural person. The definition is wide and covers someone 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, psychological, genetic, mental, economic cultural or social identity of that natural person. This means that under GDPR an IP address can be personal data.

1.2 Personal data can only be lawfully processed in accordance with the provisions of the GDPR. Processing means: "any operation or set of operations which is performed on personal data -whether or not by automated means , such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use , disclosure by transmission, dissemination or otherwise making available, alignment or combination." restriction, erasure or destruction".

2. Key Changes in the GDPR

Accountability and Governance:

2.1 GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, GDPR makes them explicit and the new accountability principle in Article 5(2) requires the Council to demonstrate that we comply with the principles and put in place a comprehensive range of enhanced governance measures.

2.1 As a consequence the Council must implement appropriate technical and organisational measures that ensure and demonstrate that we comply with Article 5. This will include the creation of several internal data protection policies, increased staff training, internal audits of processing activities, and reviews of internal policies e.g. HR policies. Relevant documentation must be maintained which we will be required to make available to the relevant supervisory authorities for investigatory purposes.

Data protection by design and data protection by default:

2.2 Under GDPR the Council has an obligation to implement technical and organisational measures to prove that the Council has considered and integrated data protection into our processing activities. We will be required to ensure and demonstrate that privacy and data protection is a key consideration in the early stages of any project which includes the following:

- building new IT systems for storing or accessing personal data;
- developing, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or

- using data for new purposes.

Data Protection Impact Assessments:

2.3 Article 35 requires a Data Protection Impact Assessment to be undertaken in order to identify the most effective way to comply with the data protection obligations and meet individuals' expectations of privacy. A Data Protection Impact Assessment will outline the description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the Council. It will evaluate the necessity and proportionality of the processing in relation to the purpose. It will assess and establish potential risks to individuals and allow the Council to put measures in place in order to limit any risks by increasing the security of the data thus demonstrating that the Council is complying with the Regulations. The DPO, will be responsible for overseeing this process.

Privacy Notices:

2.4 GDPR places an obligation on the Council to provide individuals with fair processing information in the form of a privacy notice. The current data protection provisions require the Council to inform individuals of our processing activities."

2.5 GDPR takes this further and emphasises the need for transparency over how we use personal data. GDPR sets out the information that the Council must supply and when individuals should be informed.

2.6 Specific information we must provide under GDPR includes:

- The identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer
- Purpose of the processing and the legal basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data collected or held is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

2.7 GDPR also requires further information to be placed within our privacy notices about the processing of personal data which must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

2.8 All current privacy notices will need to be reviewed and where necessary, to satisfy the conditions set out under Articles 12 and 13 of GDPR.

2.9 Work will be needed to identify any services that are currently processing personal information without appropriate privacy notices in place. This process must be documented in order to demonstrate compliance with Articles 12 and 13. The DPO will take the lead role in this area.

Records of processing activities:

2.10 In order to ensure that the Council can demonstrate that we are complying with the GDPR we must document our processing activities. This will primarily be set out within our obligation to provide comprehensive, clear and transparent privacy policies. However we must also maintain additional internal records of our processing activities. It is therefore essential that data protection audits are carried out across the Council on at least an annual basis in order to ensure we are complying with and continue to comply with GDPR.

2.11 The DPO will take the lead role in conducting these audits, liaising with the Council's Internal Audit Department when required.

A change in how we obtain consent:

2.12 The GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and an unambiguous indication of the individual's wishes.

2.13 Consent under GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes or inactivity will not constitute consent. A record must be kept of how and when consent was given. Individuals have a right to withdraw consent at any time and work is underway to review consent mechanisms to ensure they meet the standards required under the legislation.

New rights for individuals:

2.14 The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. The time limits for a response have changed. The Council will have less time to comply with a data request under the GDPR. Under Article 14 of the GDPR information must be provided without delay and at the latest within one month of receipt. Currently the Council has 40 calendar days to respond to a request from receipt of the fee. GDPR removes the £10 statutory fee for providing information.

2.15 GDPR introduces a new best practice recommendation that where possible the Council should be able to provide remote access to requests for personal data through a secure self –service system.

2.16 Key rights include:

- **The right to be informed**
  This encompasses our obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how we use personal data.

.

- **The right of access**
  Under the GDPR, individuals will have the right to obtain:
  - confirmation that their data is being processed;
  - access to their personal data; and
  - Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

- **The right to erasure:**
  The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued retention or processing.

- **The right to restrict processing**:
  Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, the Council will be able to store the personal data but will not be able to process (use) it further.

.

- **The right to rectification**:
  Individuals are currently entitled to have errors in their personal data rectified if it is inaccurate or incomplete under the DPA. However the GDPR states that if we have disclosed the personal data in question to third parties, we must inform them of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

- **The right to data portability**:
  The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- **The right to object:**
  Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

This will mean that the Council will have to implement policies and procedures to ensure that where we are processing data for the purposes listed above, individuals are given the opportunity to object and there are means for us to withdraw their data if they decide to object.

- **Rights in relation to automated decision making and profiling:**
  The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA. The Council will need to carry out a review of all our ICT systems in order to identify whether any of our processing operations constitute automated decision making. Once we have established what systems are making automated decisions we will be required to update our procedures to deal with the requirements of the GDPR.

- **New rights for children:**
  The GDPR contains new provisions intended to enhance the protection of children's personal information. Where services are offered directly to a child, the Council must ensure that our privacy notice, and any other documentation we produce relating to these types of processing activities are written in a clear, plain way that a child will understand. If the Council offers an online service to children, we will need to obtain explicit consent from a parent or guardian to process the child's data. This particular element of the GDPR may impact children's social services or education services. A review of our online presence will need to be carried out to ensure we are compliant.

  The GDPR states that parental/guardian consent for access to online services is required for children aged 16 and under (presently it is 13 and under in the UK). Online Services includes most internet services provided at the user's request. The GDPR emphasises a high level of protection where children's personal information is used for the purposes of marketing and creating online profiles.

  Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

Existing and new contractual arrangements:

3.17 All existing contractual arrangements which involve third parties processing the Council's data, must be reviewed. Recent work on the contracts register will support this.

3.18 Under GDPR specific legal obligations are placed upon Data processors, where the contractor holds and processes data on behalf of the Council (The Data Controller).

3.19 Under Article 28 GDPR Contracts must stipulate that the data processor will:

- Process only on documented instructions
- Ensure those processing personal data are under a confidentiality obligation
- Take all measures required by Article 32 GDPR to ensure a level of security appropriate to risk.
- Only use sub-processors with controller's consent
- Assist the controller in responding to requests
- Assist the controller in complying with obligations relating to security, breach notification, impact assessments and consulting with supervisory authorities
- Delete or return all personal data at the end of the agreement
- Make available to the controller all information necessary to demonstrate compliance; allow and contribute to audits, and inform the controller if its instructions breach the law.

3.20 In addition to updating the data protection clauses in contracts, other agreements, such as database access agreements, data processing agreements, data disclosure agreements and also the information sharing protocols will need to be re-negotiated in order for them to comply with Article 28.

Breach notification:

3.21 There is at present no general duty to report information breaches to the Information Commissioner. GDPR changes this and introduces a legal duty to report the majority of breaches in 72 hours. Where the breach puts the data subject at a high risk, the Council is obliged to tell the subject(s) directly about the breach and advise them as to what actions have, and, are to be taken as a result.

3.22 The most significant consequence is that of the fines. A Data Breach and failure to notify the ICO and subject within the stated time scales can result in a Tier 1 maximum fine of around £8.9m.

3.23 The Council must therefore review and strengthen its current breach notification policies and disseminate this information to all staff and members.