Appendix 1

Overview of the new requirements under the General Data Protection Regulation (GDPR)

1 Definition of "personal data".

GDPR applies to "personal data". Under the GDPR there is a more expansive definition to include such information as online identifiers e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This is wider than the DPA definition and could include chronologically ordered sets of manual records containing personal data. Personal data which has been pseudonymised e.g. key coded can fall within the scope of the GDPR depending upon how difficult it is to attribute the pseudonym to a particular individual. There is a revised definition of sensitive personal data (to which additional safeguards are required) and is now known as "special categories of personal data".

2 Data Protection Principles

Under the GDPR the Data Protection Principles set out the main responsibilities for organisations. The Principles are similar to those in the DPA with added detail in some areas. Processing of personal data must comply with all six of these Principles:

- Lawfulness fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Retention and
- Integrity and confidentiality.

The most significant change is the new Accountability principle. This will require the Council to be able to demonstrate compliance with the six Principles for example by documenting all decisions which are taken about a processing activity. The significance of this new responsibility should not be under estimated.

3 Lawful processing

For processing to be lawful under the GDPR the Council must identify a lawful basis before it can process personal data. It is important for the Council to determine the lawful basis for processing personal data and to document this. Some lawful bases which the Council has relied upon are no longer available under GDPR. The following lawful basis are available to the Council going forward.

- Consent
- Performance of a contract

- Compliance with a legal obligation
- Necessary to protect the vital interests of a data subject
- Necessary for the performance of a task carried out in the public interest.

Additional conditions apply to special categories of data (previously referred to as "sensitive personal data").

4 Consent

Requirements around consent are significantly enhanced under GDPR. There must be some form of affirmative action or in other words a positive opt in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. The Council must now include a way for people to withdraw consent. Particular care must be taken to ensure consent is freely given. Consent has to be verifiable and individuals generally have more rights where the Council rely on consent to process their data.

5 Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data. There are new rules where services are offered directly to a child and in relation to on line services to children. If consent is the basis for processing the child's personal data a child under the age of 13 cannot give that consent themselves and instead consent is required from a person holding parental responsibility.

6 Individuals' rights

GDPR both creates new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for individuals:

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

The Right of Access – often referred to as a 'Subject Access Request' is significantly revised under GDPR. The current fee of £10 is removed and the council is required to comply with this right free of charge. A "reasonable fee" can only be charged when a request is manifestly unfounded or excessive. The time period for compliance is also revised under the GDPR. A 40 day response time is reduced to "within one month" of the receipt of the request.

7 Accountability and governance

The GDPR contains provisions that promote accountability and governance. These complement the GDPR's transparency requirements. Whilst the principles of accountability and transparency have previously been implicit requirements of data protection law the GDPR's emphasis elevates their significance.

As a result the Council must put in place comprehensive but proportionate governance measures. Good practice tools such as Privacy Impact Assessments and Privacy by design are now legally required in certain circumstances.

Accountability requirements

The Council must:

- Implement appropriate technical and organizational measures that ensure and demonstrate that the Council is complying with GDPR. This is likely to include internal data protection policies, staff training, internal audits of processing activity and reviews of internal HR policies;
- Maintain 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
- Use data protection impact assessments where appropriate.

Records of processing activities (documentation)

As well as the need for detailed privacy policies as an organization with more than 250 employees additional records of processing activities are required to be maintained.

Data Protection Impact Assessments (DPIAs).

DPIAs are a tool which can help the Council identify the most effective way to comply with data protection obligations and meet individual's expectations of privacy. GDPR makes obligatory the need to carry out a DPIA when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals.

8 Breach notification

A personal data breach means a breach of security leading to the destruction, loss, alternation, unauthorized disclosure of, or access to, personal data. A breach is more than just losing personal data. The GDPR introduces new duties for the Council to report certain types of data breach to the ICO and in some cases to the individual's affected. Cases must be assessed on a case by case basis. A notifiable breach must

now be reported to the ICO within 72 hours of the council becoming aware of it. Staff must understand what constitutes a data breach. The Council's internal breach reporting procedure will need to be reviewed. There must be robust breach detection, investigation and internal reporting procedures in place in view of the new tight timescales for reporting a breach.

9 Transfer of Data

The GDPR imposes restrictions on the transfer of personal data outside the EU or third counties or international organisations.

END