Appendix 1 – General Data Protection Regulations (GDPR) Position Statement

Background

The GDPR comes into force on 25 May 2018. The Council must be compliant with the GDPR on or before this date.

GDPR is being brought in for, amongst others;

- Enhancing individual's information rights,
- Introduce a harmonious approach to data protection across the whole of the EU,
- A chance for the law to catch up with technological advancers (e.g. data analytics, biometrics etc).

GDPR introduces the following key changes:

- The definition of personal data is broader, bringing more data into the regulated perimeter
- Consent will be necessary for processing children's data
- The rules for obtaining valid consent have been changed
- The appointment of a data protection officer (DPO) will be mandatory
- Mandatory data protection impact assessments have been introduced
- There are new requirements for data breach notifications
- Data subject have the right to be forgotten
- Data processors share the responsibilities for protecting personal data
- There are new requirements for data portability Processes must be built on the principle of privacy by design

It will replace the current Data Protection Act 1998 and will be supplemented further by the Data Protection Bill that is currently passing through Parliament.

The Data Protection Bill will:

- Make domestic data protection laws fit for the digital age in which an ever increasing amount of data is being processed.
- Empower people to take control of their data.

- Support UK businesses and organisations through the change.
- Ensure that the UK is prepared for the future after we have left the EU.

GDPR provides individuals with greater control on the use of their data and introduces tighter controls on the processing of personal data. This is backed up by much stricter penalties in the form of fines. It has been described as the biggest change to data protection law for a generation.

Any use that processes personal data is affected by GDPR.

A breach of the regulations can lead to a maximum fine of €20m and this needs to be taken into consideration when determining priorities and assessing the allocation of resources.

What has been done to date?

Governance Arrangements

- Corporate Governance Board – The Council's Officer Corporate Governance Board oversees all aspects of the Council's governance arrangements and is responsible for ensuring that those arrangements are fit for purpose. This Board will hold the Information Governance Board to account – see below.

- Information Governance Board – This is the operational Board charged with implementing GDPR across the council and is chaired by the Monitoring Officer. It is made up of the council's Information Management Unit and GDPR Champions (see below).

- Project Plan – A project plan has been established that takes the Council from its inception to the 25th May 2018. The plan is owned by the Information Management Unit, who reports on progress to the Information Governance Board and managed through the Information Governance Board. The plan covers all the key steps that the Council need to go through to ensure that it is compliant with GDPR at the deadline. The Project Plan is a 'living' document and is revised to reflect changes in the understanding of the scope GDPR as it emerges and as additional issues and matters arise.

  The project plan continues past the 25th May and will deal with further changes to legislation, the continual improvement of existing process and data protection audits of existing processes.

Director - Monitoring Officer – Project Sponsor and the key link between the Corporate and Information Governance Boards and the Executive Management Team and Members.

Information Governance Manager – Project Lead and key corporate contact for GDPR across the Council. Responsible for operational co-ordinations and delivery of the GDPR Project, and directly manages the corporate Information Management Unit.

Information Management Unit

The council's Information Governance Unit supports the delivery of the GDPR Project. Its role is to:

- Deliver the GDPR project plan,
- Escalate issues within the overall project plan to EMT,
- Provide professional guidance on corporate issues,
- Attend all senior DMT to provide training and awareness on GDPR,
- Attend directorate working groups as required,
- Provide corporate training as required,
- Advise and support members on GDPR compliance
- Provide corporate templates,
- Be the centre of excellence for all GDPR (and wider Information Management) issues across the Council,
- Assist and collate in identifying all information processes within the Council,
- Arrange a central point of disseminating supporting information to the champions,
- Arrange for additional corporate resources as and when required.

As part of the role out of GRPR across Directorates, all senior management teams have been visited as well as the majority of the next tier management teams. This has re-enforced the need to keep GDPR on service's agendas and ensures that the project plan does not slip.

GDPR Champions

Each director has nominated several champions across their directorates to drive GDPR, in total there are 24 champions throughout the council.

All champions are members of the Information Governance Board and required to attends all meetings of the Board. They perform a key liaison and advisory role between the Board, Information Management Unit, their Director and team within their respective directorates.

The champions are responsible for driving GDPR across their service areas, to provide basic knowledge and understanding and to act as a focal point for the corporate team to pass relevant information down as well as a conduit for issues/information upwards.

Information Flows - A key objective for champions is to provide Information Flows for each directorate.

The council receives personal information for a variety of legitimate purposes and reasons and will use that information to discharge its powers, duties and responsibilities.

Under GDPR it is necessary to map all such information and capture the uses to which that information has been put. These information flows are vital as they will highlight:

- Current information being collected,
- Why it is being collected,
- Powers of collection (e.g. statutory requirement etc),
- Is it shared, and if why if applicable, and
- How long we keep it for.

As part of the corporate response, the champions have received external training on GDPR, as well as being supported by the Council's central Information Management Unit (IMU).

As previously mentioned GDPR only affects personal data, in reality this means that nearly all processes the Council undertakes incudes some element of personal data and will be affected by the new regulations.

Next Steps

Following on from completing the flows next steps are:

- Implement basic GDPR E-learning for all Council staff and members,

- Carry out the communication plan within the GDPR project plan to ensure that the requirements of GDPR are clearly communicated to all staff, partners and stakeholders as required,
- Inform elected members of their specific responsibilities under the new regulations,
- Identifying all forms currently being used (both physical and web) and ensure that the information being requested is necessary and proportionate,
- Updating/creating data sharing agreements,
- Creating and implementing new privacy notices,
- Reviewing existing IT systems for compliance with the new regulations and
- Reviewing all existing file stores to ensure that they are compliant with both GDPR and the approved retention scheme,
- Issue new forms that are compliant with the regulations.

Corporate Resources

The Council currently maintains a corporate team to oversee Information Governance matters, including the introduction of GDPR. As part of the GDPR plan a dedicated project manager was introduced into the corporate team to manage and oversee the project.

External professional providers have been used to provide specific training and further providers are currently being sought to provide further knowledge and assurance to ensure that the project remains on course.

A further resource is being sought for a temporary post within the corporate team to provide additional capacity and resilience. It is envisaged that this will be a for a fixed term of between 2-6 months dependent upon the needs of the service.

Challenges

The Council still has several challenges facing it to ensure that the Council is compliant by the deadline:

- The scale of the information held by a local authority ranges from simple telephone enquiries or library cards through to complex

safeguarding, council tax and electoral information – which cannot be underestimated.

- The range of IT systems and applications used across the Council that need to be compliant in considerable. Discussions are ongoing with providers and assurances being sought.

- The volume of forms that the Council uses to carry out its functions will need to be reviewed and updated as necessary to be GDPR complaint.

- The level of hardcopy information retained by the local authority will need to be reviewed in accordance with the revised retention schemes as necessary.

Elected Members

- Under GDPR, as under DPA, all elected members will be their own data controller and will have to continue to be registered with the Information Commissioner's Office,

- A predominate area of elected members work revolves around casework for constituents, and this will be classed as personal data. The handling, using and deleting of this data will be subject to the GDPR,

- A briefing paper will be prepared before end of February to be issued to all elected members covering GDPR and how it may impact upon their roles,

- A series of briefing sessions will be held in March for elected members to attend to give further information on GDPR and to answer any specific questions that elected members may have.

- Appropriate training will be provided to members at the end of March.

Position Statement

The Council is currently on track with its project plan in accordance with its scheduled deadlines. However, the size of the task cannot be under estimated and the need to remain on track is paramount.

The project is a very resource intensive and will impact upon the total level of available resources of the council. This is compounded by the tight timescales and milestones to be achieved under the Project Plan.

Matters are not helped by the uncertainty on the interpretation and scope of certain aspects of GDPR not yet being fully settled.

As such the Council's Corporate Risk Register identifies this project as a high risk and is likely to remain as such until greater certainty on compliance with GDPR can be assured.

Officers engaged with GDPR project are liaising with their trade professional bodies, regional and national colleagues and forums to keep abreast of the latest understanding and application of GDPR.