Appendix 3 - Action to Ensure Compliance.

1. GDPR Working groups and Project plan

1.1 Taking the 51 recommendations set out by the Data Protection People, a project plan has been created expanding on the recommendations and creating actionable tasks. These recommendations and tasks are organisation wide and in an attempt to get departments to adopt ownership of their own data working groups have been created in the following areas:

Adults Social Care	Children's Social Care
Public Health	Housing
Education	Finance
Planning	Environment
Regeneration	HR
Corporate Services	Commissioning & Procurement

1.2 Each group meets with the Principal Information Assurance Officer on a 4-6 week basis to review the pending legislation that will be replacing the DPA, to have and understanding and opinion of the roadmap and communications plan and to identify and understand whether, and how, corporate policy might change.

The objectives of the working groups are:

- Agree action plan and milestones on GDPR Toolkit
- To make further recommendations to the organisation for necessary policy changes and identify gaps
- Discuss the GDPR action plan and designate group members to foster ownership and help achieve specific tasks
- Increase awareness and communications across the department
- Discuss and plan communications service users
- Discuss any outstanding action points from previous meetings;
- Discuss any near misses or breaches which may have occurred in the past month and their impact if occurred post May 2018;
- Ensure the changes are imbedded and implemented post go live

Work Streams in Practice

1.3 Of the recommendations there is a clear distinction between actions that need to be taken by the Information management team; writing policies, providing a robust training framework, ensuring that the technology provided can support the business and keeping up a momentum of communications, awareness and good practice.

1.4 Actions required to be driven and supported closely by Information Management are:

- Privacy impact Assessments
- Information Sharing Agreements

- Touchpoint Disclaimers
- Process mapping
- Identification of legal basis for processing and sharing
- Aligning processes with the individual's rights
- Completing training
- Understanding of the Breaches and notification

Supplier and Third party processor engagement

1.5 Key to the success of being compliant with the GDPR and ensuring that our applications and systems support our processing practices for Information Governance and Security is the level of engagement with our suppliers and processors (those hosting our data on their infrastructure).

1.6 As part of the GDPR working group, we will be contacting current as well as potential suppliers and inviting them to provide a statement of intent on their bid to also be ready and provide a product that is compliant with the GDPR. This will challenge their development and gain valuable insights that will help us partner with responsible and competent partners.

1.7 Similar to supplier engagement, any business area that outsources/commissions another organisation to carry out data collection and/or processing on our behalf must be able to demonstrate a level of commitment to the change in law.

1.8 As Data owners, and in most instances, controllers we have a requirement to be diligent and specific as to how our third party processors handle data on our behalf. The significant issues of the law will be addressed by the contract managers and Principal Information Assurance officer and form part of the contract monitoring framework.

1.9 Challenging our supplier and third party development will help us gain valuable insights that will enable us to partner with responsible and competent associates, feeding into the requirement or privacy by design and privacy by default mandated by the law.

Commissioning, Procurement & Contract Monitoring

1.10 Work has been identified and started to provide an end-to-end process for commissioning and procurement that creates a symbiotic relationship between the business areas and information security and governance.

- Use of Privacy impact assessments at the business requirement stage
- Gateway evaluation questions
- Variations to existing contract
- Future proofed clauses for new contracts
- KPI's and monitoring framework

Legal Support

1.11 The legal division plays a crucial role in supporting the organisation towards compliance. Assisting in creating sharing agreements, disclaimers, identification of legal entities and legal basis for processing. This will ensure our business areas stand up to the necessary litmus tests to ensure the processes are aligned.

Training

1.12 Training and Awareness is an essential component of keeping the Council operating in a safe and legal manor. We currently have an Information Governance Training module on the InfoAware platform that we encourage officers to conduct every 2 years.

1.13 To comfortably meet the requirements of the new law we are seeking to add 6 modules to the portal for all officers to complete in a rolling 2 years cycle interspersed with policy acceptance. This will allow us to demonstrate by means of reports that our network users have received a comprehensive training package that has been backed-up by our policies and procedures. Beyond these Council-wide modules we have a need to provide role specific training for areas such as social work, contract managers and commissioners and Subject Access Request (SARs) coordinators.

SARS

1.14 The Council has a devolved approach to handling Subject Access and Freedom of Information requests with Individual departments. The role of coordinating and replying to them has been assigned to an existing post.

1.15 The bulk of the annual requests across the Council are concentrated in Adult's and Children's social care, handling on average 45 and 39 requests respectively. With confidence we can assert that all requests pertaining to adults are being met within the current timescales mandated by the data protection act.

1.16 An area of concern is that Children's requests are not being wholly met under the current parameters. This is due to the retrieval of boxes from TNT having an associated cost and time constraint, printing time is a constraint due to volume and there is no dedicated resource for redaction.

1.17 Under the GDPR the timescale for reply shorted from 40 calendar days to 30. We can no longer charge for requests unless deemed unnecessary or repetitive and we have to provide information on how long we keep the files for, with evidence of our retention policy. There is speculation that Subject Access Requests along with the additional rights of the individual and ability to claim compensation from the organisation could mean a significant uplift in requests with the top tier of fines being reserved for this type of failure.

Schools Awareness Program

1.18 The Council is embarking on a Schools awareness program which aims to give the relevant accountable personnel encouragement priorities and plan for an assured route to compliance without alleviating their responsibility.

1.19 The Principal Information Assurance Office is attending the School's Forum for Primary, Secondary and Special schools to present in the next half term. Present will be Head Teachers and an invitation will be extended to Data Protection Officers if required by larger schools, federations and multi academy trusts..

1.20 To support this contact, communications will be included in the schools bulletin and the Council will be compelling the schools to engage with their supplier and third party processors as an act of due diligence.