APPENDIX 1

High Level Action Plan (indicative)

Key – "pd" = personal data

	ACTION REQUIRED	NOTES
1	Resources Ensure the relevant resources to prepare for change have been allocated.	Implementing GDPR could have significant resource implications in some services in the Council, e.g. in operational delivery and at a central point in coordinating the activities and demonstrating compliance
2	Appoint a DPO (Data Protection Officer)	Must have a nominated officer to fulfil requirements of Art 37, 38 & 39
3.	Create an Art 30 Record of processing activities. To do this:	Must have comprehensive records of what personal data is held, where it came from, for what purpose, who it is shared with, the legal basis for doing so and how long it will be retained.
(i)	Carry out information audit across the Council to map data flows	Each controller shall maintain a record of processing activities which shall contain all of the following info:
(ii)	Identify legal basis for all processing activities and document this	(a) name and contact details of controller and DPO (b) purpose of processing
(iii)	Review and revise existing Corporate	(c) description of categories of data subjects and of categories of personal data

	Catalogue (may require supplementary documentation)	(d) categories of recipients to whom personal data have been or will be disclosed (e) where applicable, transfers of personal data to a third country including identification of that country and documentation of suitable safeguards. (f) where possible, envisaged time limits for erasure of different categories of data
(iv)	Review and revise existing Retention and Disposal Schedule	
(v)	Review and revise existing Data Protection Policy and ICT Policy to deal with new and revised principles and add further and mended Guidance Notes for officers.	(g) where possible, a general description of technical and organisation security measures referred to in Art 32(1)
4.	<u>Document compliance with the 6 GDPR principles ("Accountability").</u> This can be done by Art 30 records Review current processing activities and consider how can demonstrate that its processing of personal data complies with the GDPR	**<u>ART 5 – THE 6 PRINCIPLES OF DATA PROCESSING</u>** (a) **<u>'lawfulness, fairness and transparency'</u>** (b) **<u>'purpose limitation'</u>** - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (c)**<u>'data minimisation'</u>** - adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. (d) **<u>'accuracy'</u>** - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed and erased or rectified without delay. (e) **<u>'storage limitation'</u>** - kept in a form which permits

		identification of data subjects for no longer than is necessary for the purposes for which the pd are processed; pd may be stored for longer periods insofar as the pd will be processed solely for archiving purposes in the public interest, scientific research or historical research purposes or statistical purposes in accordance with Art 89(1) subject to implementation of the appropriate technical and organisational measures required by this reg in order to safeguard the rights and freedoms of data subjects. (f) **'integrity and confidentiality'** - processed in a manner that ensures appropriate security of pd including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
5. (i) (ii)	Subject Access Request Review and revise existing SAR procedure to reflect new timescales, requirements and removal of fees Create a policy on refusal of SAR requests to demonstrate criteria to refuse has been met.	 No fee* 1 month to respond 2 month extension if complex Can refuse *(although can charge reasonable fee if request is unfounded or excessive)(no guidance yet on charges although may be based on Freedom of Information regime)
6. (i)	New Data Subject Rights Update existing Data Protection Policy to	Art 12 Right to rectification

	ensure that the Council can deliver the new and revised Data Subject rights.	Right to erasure (right to be forgotten)
(ii)	Create a policy on the right of erasure and how erasure will be complied with.	Right to restriction of processing
(iii)	Update existing Data Protection Policy to deal with new and revised exemptions to the Data Subject rights.	Notification obligation regarding rectification or erasure of pd or restriction of processing Right to data portability
(iv)	Prepare standard responses for anticipated requests for each service area.	
7.	<u>Privacy Notices</u>	Must include ID of Data Controller Contact details for DPO
(i)	Prepare a corporate policy/guide for staff on privacy notices.	Purpose for processing and legal basis for doing so Legitimate interests Recipients
(ii)	Review and revise current privacy notices to ensure compliance. All documents will have to be changed.	Data transfers Retention Period (could do a link to R & D Schedule) Subject rights (inc right to withdraw consent) Right to complain to ICO
(iii)	Prepare a privacy policy for data subjects which is easily accessible	Consequences of not providing the data (statutory/contractual requirement) Automated decision making (profiling) Sources (inc public sources)
8.	<u>Consent</u>	
(i)	Review and revise all consent mechanisms (look at how seeking, obtaining and recording consent).	Must be freely given, specific, informed, and unambiguous. Must be a positive indication of agreement to personal data being processed. Cannot be inferred from silence, inactivity or pre ticked boxes.

(ii)	Amend all opt ins.	Must be separate terms and conditions
(iii)	Review and consider those situations where implied consent is used and make a decision on whether those consents will remain valid under the GDPR	If relying on consent then must be: <u>Unbundled</u> – consent must be separate from other terms & conditions.
(iv)	Create a procedure to withdraw consent at any time	Should not be a pre condition of signing up to service unless necessary for that service.
(v)	Review all documentation to make sure consent section is clearly distinguished, written in laymans terms and not comprising a condition of performance	<u>Active opt in</u> – pre ticked opt out boxes are invalid Need to use unticked opt in boxes or similar active opt in methods
(vi)	Create an effective audit trail for consents	<u>Granular</u> – give granular options to consent separately to different types of processing wherever appropriate <u>Named</u> – name your organisation and any third party who will be relying on the consent – even precisely defined categories of third party organisations will not be acceptable under GDPR <u>Documented</u> – keep records demonstrating what the individual has consented to including what they were told and when and how they have consented. (doesn't have to be written, can be verbal but must be recorded) <u>Easy to withdraw</u> – tell people they have the right to withdraw their consent at any time and how to do this. It must be as easy to withdraw as it was to give consent. Will need to have simple and effective withdrawal mechanisms in place. <u>No imbalance in the relationship</u> – consent will not be freely

		given if there is an imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers who should look for an alternative lawful basis.
9.	<u>Legitimate Interests</u> Review and revise all situations where legitimate interests are used and consider how this can be amended to ensure compliance with GDPR	Not likely to be relevant to the Council
10. (i) (ii) (iii) (iv)	<u>Contracts</u> Assess & review all on-going data sharing agreements with a view to ensuring compliance by the data processors. If consent section then will need to review Review list of all contracts with data processors Amend contracts with data processors to include all Art 28(3) requirements May require renegotiation because of extra obligations Prepare corporate guide for staff when	Data Processor must offer sufficient guarantees. Art 28(3) Contract must include: 1.act only on DCs instructions 2. nature of processing, data, subjects 3. ensure confidentiality commitment 4. all necessary security measures 5.respects conditions for choosing another processor 6.assist DC with subject's rights security and risk assessment 7. supply information and allow audits 8. delete or return data

	choosing a Data Processor.	
11. (i) (ii) (iii) (iv) (v)	<u>Security</u> Review and revise current technical and organisational methods to ensure compliance. Review and revise existing ICT Security Policy Are security measures appropriate to risks involved? Review and revise existing disaster recover policy? Create a policy/guide on Pseudonymisation of data	Art 32(1) taking into account the state of the art, costs of implementation, nature, scope, context and purpose of processing as well as the risk of varying likelihood and severity of rights and freedoms, controller shall implement appropriate technical and organisation measures to ensure a level of security appropriate to the risk including as appropriate: (a) pseudonymisation and encryption of personal data (b) ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.
12. (i) (ii)	<u>Data Protection Impact Assessments</u> Carry out DPIAs for those areas of operations which present a potential high risk. Create a policy/guide to assist staff to understand when they must conduct DPIA and put a process in place to action this.	Art 35 - Where processing is likely to result in high risk to the rights and freedoms of natural persons then must carry out DPIA before processing. Art 35(3) Specific requirement to do DPIA in some circumstances. Art 35(7) sets out content Need to include ID of Data Controller

(iii) (iv)	Link DPIA framework to existing risk management and project management processes Establish and make public a list of the kind of processing operations which are subject to the requirements of DPIA and communicate the list to the senior management Compliance with approved codes of conduct shall be taken into due account in assessing the impact Art 35(8) If risk is high then must consult with ICO before processing	Contact details for DPO Purpose of processing and legal basis Legitimate interests Recipients Data transfers Retention period (can do link to R & D Sch) Subjects rights Right to complain to ICO Consequences of not providing data (statutory/contractual) Automated decisions Sources Must be easily accessible Can have a general one with more info on website Art 36(1) specific requirements Art 36(3)
13. (i) (ii)	<u>Profiling</u> Conduct a review and assessment of all data activities that may qualify as profiling and determine what steps it needs to take to meet the requirements of the GDPR If so, must tell people in our privacy notices Create a policy/guide on the right to object to automated decisions were has significant affect	Art 22 – any form of automated processing of personal data consisting of the use of pd to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning a naturals persons performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Right not to be subject to a decision based solely on automated processing (human intervention) which significantly affects him. Exceptions: necessary for entering into a contract Authorised by law Data Subject given explicit consent
14	<u>Training and awareness</u>	All staff must be aware of GDPR requirements and how they

	Train staff on new data protection responsibilities under the GDPR	affect them in doing their job
15. (i) (ii)	<u>Special Categories</u> Conduct an assessment of all data it processes which might be considered 'special categories of data' Create a policy/guide to determine what steps it needs to take to meet the requirements of the GDPR	 Sensitive PD is now Special Categories Prohibition unless specific reason Don't ask for it unless really need it.
16. (i) (ii) (iii)	<u>Breach Procedure</u> Review and revise existing procedure for managing data breaches to include detecting, assessing, reporting and investigating breaches and for notification of breach to ICO. Create guide on when to tell data subject about a breach and procedure for doing so. Prepare a guidance note on the remedies, liabilities and penalties.	Art 33 – controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the breach to the ICO unless the breach is unlikely to results in a risk to the rights and freedoms of natural persons. Where not made within 72 hours must be accompanied by reasons for the delay. If doesn't involve risk to individual then don't have to report. If doesn't involved high risk then report to ICO within 72 hours If high risk to ICO and data subject without undue delay

		Art 34 – when breach is likely to result in a high risk to rights and freedoms of natural persons, must tell data subject without undue delay subject to some exceptions.
17.	<u>New offences.</u> Prepare a guidance note on the new offences	Intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data, and knowingly handling or processing such data Altering records with intent to prevent disclosure following a subject access request Retaining data againt the wishes of the data controller (offence by processor)
18. (i) (ii)	<u>ICO</u> Undertake a review of current arrangements with ICO Prepare a guide for staff on the investigative and corrective powers of the ICO	Art 58
19. (i)	<u>Transferring data abroad</u>?. Review current processing activities to ensure no breach of Art 44.	Art 46 safeguards Is a list of countries that has adequate protection USA – if using privacy shield then ok (subject to compliance with management of the arrangement)

(ii)	Prepare a guide policy on transferring data abroad	
20.	<u>Children and Consent</u> Put policy in place to verify individuals ages and to gather parental or guardian consent for the data processing activity	The proposed Act (Bill) will allow a child aged 13 years or older to consent to their personal data being processed