	GDPR 12 Steps Assessment				
	Red — Not met and no plan to meet in place		RAG	**Complete/progress**	**Outstanding/Ongoing Improvements**
	Amber — Plan to meet in place				
	Green — Met				
1	**Awareness** Ensure decision makers and key people are aware the law is changing.	Council Members, EMT and OMT aware. Project group established with representatives from all teams.	G	Already in place at time of last council meeting Training was done with representatives from departments to make them aware that GDPR was coming into force	Formalise Data Champion role – work with Champions to raise awareness across organisation and train staff. Plan to train Council members. Plan to train Fitness to Practise Panel members (March training dates) Regular GDPR training is planned with staff both as an online exercise annually and bespoke training for the departments.
2	**Information you hold** Document the personal data you hold and with whom you share it.	We already have a Records Management Policy and an Information Asset Register. Each team has started a detailed personal data mapping process.	A	Mapping process complete SSSC Overarching Data Protection Policy updated.	Add new column for special category data. Await implementation of CMS and then work with teams to clean up existing data.

					Reinstate annual audits once Data Champions in place.
3	**Communicating Privacy Information** Review privacy notices and plan for making changes prior to implementation.	Plan in place to review privacy notices once data is mapped and lawful basis for processing identified.	G	Privacy Policy published	Consider how Privacy Policy can be improved and make improvements in line with website updates. Consider if there are any outstanding areas of the Privacy Policy which may need to be rectified, including: • Profiling • Finance Tonepay system • Recorded phone calls • HR section Add children's data.
4	**Individuals' Rights** Review procedures to ensure they cover the rights individuals have such as the rights to be informed, have access, rectification, erasure, to restrict processing, data portability, to object and not to be subject to automated decision-making.	Review of procedures planned once all data is mapped and lawful basis for processing identified.	A	Staff procedure for right to erasure and right to rectification drafted. Situations where we rely on consent complete – one mailing list.	Staff procedure for rights to erasure and rectification to be published for all staff. Non-staff - consider obligations about informing people of their right to erasure and rectification and whether an update to the website is required.

5	**Subject Access Requests** Review procedures to meet new timescales and provide more detailed information	Plan in place to review process and assess capacity to meet new timescale.	G	Currently meeting timescales Website, form and template response letter updated.	Undertake improvement science project for internal SAR process – scheduled date to undertake project in November.
6	**Lawful Basis for Processing Data** Identify the lawful basis and update your privacy notice to explain it	Plan in place to identify lawful basis once mapping of data is complete. Will need to consider length of time we retain the data for and the need to ensure that organisations we share the data with are GDPR compliant.	A	Lawful basis identified and explained in policy Procurement contacted all organisations that we have a contract with, which involves processing data on our behalf, to confirm they are compliant.	Retention schedule to be published in policy. On hold until review which is pending till completion of child abuse inquiry.
7	**Consent** Review how you seek, record and manage consent. Refresh existing consents now if they don't meet the GDPR standard	Plan in place for reviewing consents once all data is mapped.	G	One mailing list identified as requiring consent. Email sent to advise individuals on mailing list that unless signed up again they would be removed from list. Communications will manage consent.	Reviewing Registration application form to consider how consent is currently obtained. Review: • Employment contracts • Finance • L&D event attendance Lists
8	**Children**	Plan in place to review the applicability of these provisions to	A		More info needed and form of

	Ensure you have a system in place to verify ages and obtain consent if necessary.	the SSSC's work.			words Consider whether we ever seek consent in relation to bursary applications.
9	**Data Breaches** Ensure you have procedures in place to detect, report and investigate a personal data breach	Plan in place for reviewing and refreshing procedures and training.	G	Complete. Guidance for normal and severe on intranet. Developed traffic light system for how we categorise. Risk Assessment form to consider reporting to the ICO complete.	Draft data breach reporting procedure and guidance around 'near misses' and 'data security incidents'. Create flowchart to determine full route for dealing with reported data breaches. Create outcome letter for MOPs who report breaches.
10	**Data Protection by Design and Data Protection Impact Assessments** Start assessing the situations where it will be necessary to conduct a DPIA.	Applies at the deployment of new technologies and therefore will likely be relevant to the implementation of new systems such as case management. Plan in place for creating templates and training staff.	G	Template created and sat in on a few first attempts to complete by depts. Guidance developed for staff about when they should be carrying out a DPIA and uploaded to intranet.	Continue to monitor any changes to processing of data to decide when these should be carried out.

| 11 | **Data Protection Officers (DPO)**

Designate someone to take responsibility for data protection compliance. | Head of Legal and Corporate Governance. | G | Already in place at time of last council meeting | |
| 12 | **International**

Applies when an organisation operates in more than one EU member state. | N/A | N/A | N/A | |