Action as recommended by ICO			Date Completed
Action Ongoing	**Position as at 9/8/17**	**Position Sep 17 (Working Group 12 Sep)**	
Your business has implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities	Technical measures to be incorporated have been discussed with Hytech, the Council's information security technical consultants. Notices have been published to all staff on the changes on how they may affect them. Policies & Procedures will be updated during early 2018.		
Your business understands when you must conduct a DPIA and has processes in place to action this.	This was instigated at CBC during 2016. A campaign to repromote this has been commenced with email reminders sent to Directors and AD's for cascading down to Managers and Staff		
Your business has a DPIA framework which links to your existing risk management and project management processes.	This was instigated at CBC during 2016. A campaign to repromote this has been commenced with email reminders sent to Directors and AD's for cascading down to Managers and Staff		
Your business has designated responsibility for data protection compliance to a suitable individual within the organisation.	Information Security Manager who feed issues into the Information Assurance Group. This is then reported to Corporate Management Team on a quarterly basis.		
Your business has appointed a Data Protection Officer (DPO) if you are: (LIST) a public authority or you carry out large scale monitoring of individuals or you carry out large scale processing of special categories of data or data relating to criminal convictions and offences.	This is to be confirmed by the Chief Executive.		
Your business supports the data protection lead through provision of appropriate training and reporting mechanisms to senior management.	Data protection and information security training will be reviewed early in 2018 with L&D to consider changes that need to be made to it and consider more specialised training for those areas where sensitive personal data is handled more extensively.		
Your business has reviewed the various types of processing you carry out. You have identified your lawful basis for your processing activities and documented this.	We have a lawful basis for processing, although we will study the new data protection bill for any new requirements.		
Your business has explained your lawful basis for processing personal data in your privacy notice(s).	SD and MD LGSS will be working on a new draft privacy notice during August		
Your business has documented what personal data you hold, where that data came from and who it is shared with.	This will be considered by SD and CAG. Will take advice from Internal Audit on how best to do it		
Your business has planned to conduct an information audit across the organisation to map data flows.	Will speak to Internal Audit on this		
Your business has reviewed how you seek, record and manage consent.	MD LGSS and SD will be working on new consent notices for all departments shortly		
Your business has reviewed the systems currently used to record consent and implemented appropriate mechanisms in order to ensure an effective audit trail.	SD to speak to Hytec (Information Security technical experts) regarding this.		

Decision makers and key people in your business are aware that the law is changing to the GDPR and appreciate the impact this is likely to have.	Yes. CMT and Members have been made aware of the changes and there likely effect.		
Your business has identified areas that could cause compliance problems under the GDPR and has recorded these on the organisation's risk register.	We are working with Internal Audit on this		
Your business is raising awareness across the organisation of the changes that are coming.	Regular updates have been published in local media (Staff Central, Managers Emails) since the beginning of 2017. More detailed information on the changes coming is now being directed at Directors and AD's.		
Your business has set out the management support and direction for data protection compliance in a framework of policies and procedures.	We already have this in place. All policies and procedures will be reviewed early in 2018 to assess the need for change to reflect the new regulation.		
Your business monitors compliance with data protection policies and regularly reviews the effectiveness of data handling and processing activities and security controls.	Policies are reviewed every two years currently. All our information governance policies will be reviewed early in 2018 and amended to reflect the new regulations. These will only be published generally once GDPR is law. Our training package is being reviewed in conjunction with L&D beginiing in Jan 2018.		
Your business has developed and implemented a needs-based data protection training programme for all staff.	See above. This will be developed with L&D colleagues from Jan 2018.		
Your business has documented what personal data you hold, where that data came from and who it is shared with.	All our information sharing arrangements are documented and must be approved by an authorisation group consisteing of Caldecott Guardian, LGSS Corporate Lawyer, Information Security Manager and Records & Risk Officer. We will need to check how personal data holdings are recorded.		
Your business has planned to conduct an information audit across the organisation to map data flows.	We will need to consult Internal Audit on this.		
Your business has checked your procedures to ensure that you can deliver the rights of individuals under the GDPR.	This action is ongoing		
Your business has reviewed your procedures and has plans in place for how you will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR.	We will be working on this from Jan 2018. The system we have will be easy to change and we will ensure that all users are aware of the changes in plenty of time prior to implementation.		
Your business has reviewed your procedures and has plans in place for how you will provide any additional information to requestors as required under the GDPR.	Our system is already very robust and will require minimal alteration.		
Your business has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively.	These have been in place for two years.		
Your business has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage, e.g. through identity theft or confidentiality breach.	The Information Security Manager is notified of all breaches and will make an assessment on each incident on what action needs to be taken.		

Your business has mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.	See above. Information Security Manager, sometimes in consultation with LGSS, will assess if this action needs to be completed.		
If your business offers services directly to children, you communicate privacy information in a clear, plain way that a child will understand.	MD LGSS and SD will be looking at this shortly		
If your business offers 'information society services' directly to children, your business has systems in place to verify individuals' ages and to obtain parental or guardian consent where required.	Information Society services are defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of the recipient for services". This is normally taken to refer to social media or games. Further investigation to take place to see if CBC provides any services that might still come within the definition		
If your business operates in more than one EU member state, you have determined your business's lead supervisory authority and documented this.	Not applicable		