NHS Dorset CCG Action Plan

Implementation of the General Data Protection Regulation by 25 May 2018

ICO Preparing for the GDPR - 12 steps

1.	**Awareness and Accountability**			
	• Paper to Governing Body on GDPR and upcoming changes and resource implications for the CCG.	8/8/17	JG	Complete
	• Add all GDPR compliance risks to the CCG Risk Register	30/9/17	JG	Risk that the CCG will not meet its requirements under GDPR. Risk ref Q028.
	• Include GDPR information in quarterly briefings to the Governing Body and Audit and Quality Committee.	Ongoing	JG	In Progress
	• Include GDPR in annual mandatory IG training to ensure staff awareness.	Ongoing	JG/HW	In Progress
	• Set up GDPR working group with IG leads, for implementation of GDPR work programme.	Ongoing	HW	In Progress
	• Provide regular reports to the IGG for monitoring of progress of GDPR work programme and ensuring communication to teams.	Ongoing	JG/HW	Action plan to go to each IGG
	• Review all IG and internal Workforce processes to ensure they cover the accountability and governance provisions of the GDPR and promote transparency e.g. staff training, fair processing statements, consent forms etc.	31/1/18	JG/HW	In Progress
2.	**Information you hold**			
	• GDPR working group to audit directorate records and ensure deletion of PCT information where appropriate.	31/12/17	GDPR W/G	In Progress
	• Set up meeting with IT re assistance with the identification of personal data in records held by the CCG, including spreadsheets and databases.	31/1/18	DA	In Progress

	• Carry out thorough review and update of CCG data mapping to check accuracy, including where the information came from and who it is shared with. Check legal basis for all processing of personal information.	31/12/17	IG Team	In Progress
	• Update data mapping sheets to include retention dates for personal information.	31/1/18	HW	To be added once mapping complete.
	• Cross reference data mapping to the CCG Privacy Notice on the website to ensure all processing activities are recorded.	30/4/18	JG/HW	In Progress
3.	**Communicating privacy information**			
	• Review ICO's Privacy Notices Code of Practice to ensure the CCG Privacy Notices comply with this.	30/4/18	JG/HW + Comms	In Progress
	• Print out of ICO notification to ensure all information is included in new Privacy Notice.	30/4/18	JG/HW + Comms	To be undertaken on completion of previous 2 bullet points
	• Set up meeting with Comms team to discuss change of Privacy Notice on website to a layered approach. Discuss requirement to ensure the information is more descriptive about what we do with our information and the grounds for collecting this data. Notice needs to be provided in concise, simple, easy to understand and clear language, with sub-sections including: - name and details of CCG and DPO (also any other controllers and our representative); - what we process; - why (purposes of the processing); - description of the categories of individuals and categories of personal data; - categories of recipients of personal data; - details of transfers to third countries including documentation of the transfer mechanism safeguards in place; - your rights (such as right to complain to ICO); - sharing with third parties; - retention periods (i.e. in accordance with our data retention policy available on our website); - description of technical and organisational security measures; - legal basis (see section 6);	30/4/18	JG/HW + Comms	Meeting held 10 Oct with Comms. Subsequent meetings held with IG team and work underway to define layout of website.

	- right to complain to ICO.			
	• Discuss with Comms team how to ensure privacy notices are put in front of everyone we engage with, consider use of email footers with links to further information.	30/4/18	JG/HW + Comms	To be undertaken on completion of previous bullet point
	• Document where else in the CCG that Privacy Notices are used e.g. CHC. Review and update all of these as above.	30/4/18	JG/HW + Comms	Meeting with RW to look at CHC privacy notices – arranged for 5 Dec.
4.	**Individuals' rights**			
	• Produce a list of individuals' rights under the GDPR (include in revised SAR procedures): - the right to be informed; - the right of access; - the right of rectification; - the right to erasure; - the right to restrict processing; - the right to data portability (only applies to personal data an individual has provided to the CCG, where the processing is based on the individual's consent or for the performance of a contract, when processing is carried out by automated means); - the right to object; and - rights in relation to automated decision making and profiling.	31/12/17	JG/HW	List of rights produced, to be added to SAR procedures when updated.
	• Review procedures for all CCG systems containing personal data to ensure they cover the above rights, including deletion of personal data – how to locate and delete, and who authorises. Procedures also need to cover data portability, providing data in a structured, commonly used and machine readable form.	28/2/18	IAO's	Not started
5.	**Subject access requests**			
	• Review and update CCG Subject Access Procedures contained within the IG Policy to ensure new rights for individuals under the GDPR are included. Need to consider timescale, list of reasons for refusing to comply with SAR and associated policies, how to advise of data retention periods, information leaflet on the right to have inaccurate data corrected, legal basis for processing personal data, providing the information free of charge. Document new exemptions.	31/12/17	HW	In progress

	• Ensure new timescale for SAR's of one month instead of 40 days is added to Ulysses.	30/9/17	HW	Complete. We update Ulysses as required on 25 May.
	• Consider how the 'right of portability' for each system (when data obtained by consent or contractually) and the 'right to be forgotten' will be managed – include in procedures. Need to link with system owners for this one (section 4).	28/2/18	IAO's/JG	Not started
6.	**Legal basis for processing personal data**			
	• Carry out review of CCG data mapping (see bullet point 3, section 2).	31/12/17	IG Team	In progress
	• Ensure the Privacy Notice explains the CCG legal basis for processing personal data, and ensure the procedures for answering a SAR include legal basis.	30/4/18	JG/HW + Comms	Not started – dependent on results identification of all data held
	• Produce a list which sets out the conditions that can be used as legal basis under the GDPR, and ensure that the data mapping for each directorate maps to one of these conditions.	30/9/17	HW	Complete
7.	**Consent**			
	• From data mapping exercise, highlight where consent is used as a legal basis. Consider whether a different lawful basis for processing may be more appropriate	31/12/17	JG/HW	In progress
	• Where consent is used as a legal basis, review existing consent forms to ensure the consent meets the standards required by the GDPR: - specific, informed and unambiguous; - consent requests must be separate from other terms and conditions; - must be active opt-in (pre-ticked opt-in boxes are invalid), use un-ticked opt-in boxes; - give granular options to consent separately to different types of processing wherever appropriate; - must include name of CCG and any other third parties who will be relying on consent (even precisely defined categories of third party organisations will not be acceptable under the GDPR);	28/2/18	JG/HW	Take from data mapping (plus email to IG leads)

	- keep records to demonstrate what the individual has consented to, including what they were told and when and how they consented; - it must be as easy to withdraw consent as it was to give consent, people must be told that they have the right to withdraw their consent at any time. • If the consent form is not compliant with GDPR, update or stop processing.			
	• Produce a guidance sheet for staff on consent (using ICO's consent guidance document), covering collection and recording of consent. NB: right of portability only applies if your data has been collected with consent or contractually.	28/2/18	JG/HW	Not started
	• Review processes for demonstrating that consent has been given i.e. audit trails.	28/2/18	JG/HW	Not started
	• Produce documentation for IG team and IG group: - old DPA principles compared with new GDPR principles; - new conditions for processing personal and sensitive data; - applicability; - SAR exemptions.	30/9/17	JG/HW	Complete
8.	**Children**			
	• Review systems within CHC for verifying individuals' ages and gathering parental/guardian consent for the data processing of anyone under 13.	28/2/18	RW	Not started
	• Ensure the above is covered in the CCG Privacy Notice on the website (in a language that children will understand).	28/2/18	JG/HW	Not started
	• Highlight directorates where services are offered directly to children, and review privacy information to ensure it is written in a clear, plain way that a child will understand.	28/2/18	JG/HW + GDPR W/G	Not started
9.	**Data breaches**			
	• Liaise with risk team to review Incident Reporting Procedures, and ensure that the right procedures are in place to detect, report and investigate a personal data breach under the GDPR.	15/3/18	JG/SL + Risk	Meeting arranged with SH for 8 Jan 2018.
	• Update AIRS form with more specific questions relating to information risk.	15/3/18	JG/SL + Risk	As above.
	• Document which types of information would fall within the notification requirement if there was a data breach and put together incident response plan for high risk data breaches. Advise Governing Body of potential requirement for a fund to be in place for claims.	15/3/18	JG/HW	As above.

	• Ensure everyone aware of the requirement to report to ICO within 72 hours of breach, and to data subjects as well if likely to cause harm.	15/3/18	JG/HW	As above.
	• Check CCG insurance re cyber breaches – ensure insurance is not invalidated.	15/3/18	CL	To discuss
10.	**Data Protection by Design and Data Protection Impact Assessments**			
	• Review and update of PIA procedures and align with ICO Privacy by Design Guidance.	31/10/17	HW	Await Pan Dorset IG Group PIA before updates can be made.
	• Produce guidance for staff on when a PIA should be carried out, examples of when the ICO should be consulted, privacy by design and data minimisation approach (possibly include with PIA procedures).	31/10/17	JG/HW	As above
	• Place on intranet, issue to staff – contracting need to consider in context of public tenders.	31/10/17	JG/HW + DW	As above
	• Review of all existing contracts to ensure they are GDPR compliant.	31/1/18	JG/DA + DW	In progress
	• Add to Confidentiality: Staff Code of Conduct – this needs updating.	28/2/18	DA/SL	Not started
	• Link with PMO to ensure privacy by design and PIA's are included in all project templates.	28/2/18	RB/SO'F	Complete
11.	**Data Protection Officers**			
	• Compile list of requirements for DPO.	8/8/17	JG	Complete
	• Agree where DPO role will sit within CCG structure and governance arrangements – include review of IG structures.	30/4/18	SS	In progress
	• Appointment of DPO who can take proper responsibility for data protection compliance and who has the knowledge, support and authority to do so effectively.	30/4/18	SS	In progress
12.	**International**			
	• Applicability – review all processing of personal data on systems. Document who is data processor and who is data controller.	To be decided		Not started
	• Review contracts and ensure there is a written mandate setting out the obligations of the processor and the controller, and what will happen to the data at the end of the contract etc.			Not started

	• Applicability - document all systems where the processing of personal data is not carried out in the EU and ensure that there is a representative designated in writing, where applicable.			Not started
	• Determine where model contract clauses are required.			Not started