Summary of GDPR themes and implementation progress

This table presents a summary of the required actions in respect of teach GDPR theme, the current Care Inspectorate status, and planned Care Inspectorate tasks. As the Data Protection Bill continues its legislative passage, and as our general information governance improvement programme continues, these tasks will be updated and refined.

Work is now on-going with our information governance consultants to plan a clear timetable to complete the following actions over the next 5 months

GDPR Theme	Summary of required actions	Current CI status	Next CI tasks
GDPR Awareness	Ensure decision makers and key people in the organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.	Multiple references to GDPR in information governance improvement programme; discussion at Board, Audit Committee, and Senior Management Team.	Development of GDPR action plan and regular reporting of progress to Executive Team through appropriate mechanisms
Governance Structure	Appoint a Data Protection Officer (DPO) in an independent oversight role	Advice on skill and independence requirements has been obtained.	Executive Team to agree appointment.
	Maintain roles and responsibilities for individuals responsible for data privacy (e.g. Job descriptions)	Senior Information Risk Officer and Information Asset Owners (IAOs) identified and role profiles issued.	Further responsibilities will be set out in the revised Data Protection Policy.
	Ensure regular communication between the privacy team and others responsible / accountable for data privacy	Initial briefings for IAOs has commenced. Revised intranet presence for staff to see.	Effective communication and training arrangements will be in place to support IAOs.
Personal Data Audit, Register & Risk Assessment	Carry out personal data audit and use to develop and maintain an inventory of personal data holdings (what, why and how personal data is held and processed)	Information Asset Register has been agreed and will identify assets containing personal data. This will trigger more detailed personal data auditing were necessary.	Create checklists /actions for reviewing each element against GDPR requirements; pilot personal data audit and data flow template for priority areas.
	Identify the lawful basis for processing activities in the GDPR, document it and update privacy notice to explain it.	The information asset register template supports this activity.	Completion of the register will ensure the lawful basis for processing is clear and communicated.
	Conduct an Enterprise Privacy Risk Assessment	An information risk register has been developed and populated with key privacy risks	Privacy risks related to specific information assets will be identified as part of Information Asset Register.

GDPR Theme	Summary of required actions	Current CI status	Next CI tasks
Data Privacy Policy embedded across organisation	Update data protection policy framework to meet GDPR requirements and embed across the organisation.	The current Data Protection Policy was published in 2014 and requires significant review and associated implementation.	Work to review this is being led by the Care Inspectorate's information governance consultants and will be agreed by the Executive Team in the first half of 2018.
Training and awareness	Develop and maintain a training and awareness programme	SIRO training delivered, initial IAO training underway	Role based data-protection training and competencies will be developed and rolled out.
Communicating privacy information to data subjects	Maintain a data privacy notice that details the organization's personal data handling practices; Provide data privacy notice at all points where personal data is collected	Generic core privacy notice is drafted.	Publish generic notice and update core notice with sections specific to each data subject group to meet GDPR requirements.
Consent	Where lawful basis for processing is consent, review how the organisation obtains, records and manages consent and whether any changes need to be made. Refresh existing consents if they don't meet the GDPR standard.	Initial work has commenced.	Further work will be led the Care Inspectorate's information governance consultants.
Children	For processing of personal data related to children, consider if systems need to be put in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.	Not commenced.	Work will be led the Care Inspectorate's information governance consultants.
Third party sharing & data processors	Update MOUs and information sharing agreements with 3rd parties - eg external partners, fellow regulators etc.	Information Asset Register is identifying 3rd party sharing.	Liaise with appropriate parties to review and update.
	Update procurement/ commissioning procedures and review existing contracts and data processing agreements with all 3rd parties processing personal data to meet GDPR requirements	Information Asset Register is identifying 3rd party data processors and initial work has commenced.	Work to review procurement and those with commissioning responsibilities across the organisation will be concluded, to review and update requirements and arrangements.

GDPR Theme	Summary of required actions	Current CI status	Next CI tasks
Subject Access Requests	Update procedures and plan how the organisation will handle requests within the new timescales and provide any additional information.	Subject access procedure and form have been updated and incorporated in new privacy notice	Management oversight to ensure that new timescales are adhered to.
Individuals' rights	Ensure procedures cover all the rights individuals have, including requests to opt-out of, restrict or object to processing, updating / correcting their personal data, right to erasure & portability.	Measures already in place across the organisation to meet current DPA requirements.	Identify processing purposes for which the various rights are applicable; review gaps in existing procedures and update.
Organisational and technical security measures	Integrate data privacy into an information security policy.	ICT security policy updated in December 2017.	Further improvements to be considered during 2018.
	Ensure adequate organisational and technical security measures are in place (e.g. intrusion detection, firewalls, monitoring, personal data encryption, data access restrictions, security testing etc…)	Existing measures already in place.	Existing controls will be reviewed against GDPR and IG requirements informed by privacy audit and information risk work.
	Identify on-going privacy compliance requirements, e.g., law, case law/precedents, regulator codes and guidance, organisational policy, etc.	Not started, but effective policy and parliamentary monitoring arrangements are in place.	Put monitoring mechanism in place for external operating environment.
Data breaches	Ensure the right procedures are in place to detect, report and investigate personal data breaches.	New incident management procedure now agreed and in use (this supports meeting new timescales); advice provided to Information Asset Owners; incident log in place.	Review approaches ahead of May 2018 to ensure compliance with nascent legislation. Further training to be provided to a wider range of staff.
Data Protection by Design	Integrate Privacy by Design into organisational change and project management processes using Data Protection Impact Assessments for high risk processing.	Not started	Develop Data Protection Impact Assessment (DPIA) template based on ICO Code of Practice and Article 29 guidance; pilot for product development under business/digital transformation programme.
	Ensure personal data captured is adequate but minimum required for processing purposes.	Not started	Create personal data checklist to ensure personal data capture is sufficient to support the purpose but only captures

GDPR Theme	Summary of required actions	Current CI status	Next CI tasks
			minimum personal data to support the processing purpose.
Monitoring and evidencing compliance	Ensure documentation is created and retained as evidence to demonstrate accountability and compliance; conduct self-assessments of privacy management	Work already undertaken helps in building compliance documentation.	Checklist of compliance requirements will be developed including evidence column as part of IG improvement programme.