Guidelines for GDPR compliance in schools/ETBs

Heading	Action Points	Date for Action	Date for Review
Data Retention and Accountability	Review all personal data the school currently holds and determine whether or not it is held in accordance with the GDPR.		
	Make an inventory of all personal data held by the school/ETB and examine it under the following headings:		
	Why is it being held?		
	How was it obtained?		
	Why was it originally gathered?		
	How long will it be retained?		
	How secure is it, both in terms of encryption and accessibility?		
	Is the data ever shared with third parties and on what basis might this be done?		
Basis for processing data	Identify and document the legal basis for processing personal data		
	Draft or update the schools/ETBs privacy notice to explain legal basis		
	Communicate Privacy Notice to relevant stakeholders		
Data Retention times	Have an up-to-date data retention schedule in place		
GDPR Obligations	Schools/ETBs should familiarise themselves with their obligations under the GDPR and take steps to ensure compliance		
Training	Ensure staff are effectively trained in the new policies & procedures.		

Rights	Ensure that data subjects are informed of their rights under the GDPR		
	the right to be informed		
	the right of access		
	the right to rectification		
	the right to be forgotten		
	the right to restrict processing		
	the right to data portability		
	the right to compensation & liability		
Subject Access Requests (SARs)	Update policies and procedures for processing data access requests		
	Put in place a clear procedure and checklist/timeline for responding to SAR's		
	The school/ETB is obliged to confirm the identity of individuals making a SAR.		
Consent	Check processes and records in detail to be sure existing consents meet the GDPR standard		
	Communicate additional information to stakeholders in advance of processing, including:		
	the legal basis for processing the data,		
	retention periods		
	the right of complaint where data subjects are unhappy with the implementation of any of these criteria		
	whether their data will be subject to automated decision making		
	their individual rights under the GDPR		
	Records must be kept of how and when consent was given.		
Processing Children's Data	Review and update procedures for processing children's data		
	Systems in place to verify age.		

	Obtain parental or guardian consent for any data processing activity where a child is under the age of consent		
Security	Review security measures to ensure they meet the requirements of the GDPR		
	Review and refresh children's consent at appropriate milestones		
Data Breach Response Plan	Review and revise your schools/ETBs data breach incident response plan		
	Set out the incident report team responsible for dealing with a breach		
	Mandatory breach reporting done within 72 hours, as per GDPR guidelines		
	Notify data subjects where the breach is likely to result in a 'high risk' to them		
	Document any data breaches, comprising the facts relating to the personal data breach.		
Privacy by Design	Ensure the school/ETB only collects data absolutely necessary for the completion of its duties (data minimisation)		
	Limit the access to personal data to those needing to act out the data processing		
	Perform 'privacy impact assessments' for any actions that may pose a high risk for data subjects' privacy rights		
Data Protection Impact Assessment (DPIA)	The school/ETB must assess the impact of the envisaged processing operations on the protection of personal data		
	DPIAs shall be conducted where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons		
Data Protection Officer (DPO)	Consider whether schools are required to appoint a DPO		

Processing Agreements	Review and if necessary renegotiate agreements which involve the processing of personal data		
Policies & Procedures	Schools/ETBs should review their policies & procedures and update them to comply with the GDPR		