

Action Plan to achieve GDPR compliance

Heading	Action points	Date for action	Date for review
GDPR obligations	Schools familiarise themselves with their obligations under GDPR and take steps to ensure compliance	March 2018	
Data retention and accountability	Review all personal data the school currently holds and determine whether or not it is held according to GDPR	May - June 2018	
	Make an inventory of all personal data held by the school and examine it under the following headings:		
	Why is it being held?		
	How was it obtained?		
	Why it was originally gathered?		
	How long has it been retained?		
	How is it secure?		
	Is the data ever shared with 3 rd parties and on what basis might this be done?		
Basis for data processing	Identify and document the legal basis for processing personal data	May - June 2018	
	Draft or up-to-date the school's 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	May 2018	
Training	Ensure staff and governors are effectively trained in the new policies and procedures		
Rights	Ensure that data subjects are informed of their rights under GDPR	May - June 2018	
	The right to be informed		
	The right of access		
	The right of rectification		
	The right to be forgotten		
	The right to restrict processing		
	The right to data portability		

	The right to compensation and liability		
Subject access requests (SARS)	Update policies and procedures for processing data access requests	May - June 2018	
	Put in place a clear procedure and checklist/timeline for responding to SARS		
	The school is obliged to confirm the identity of the individual making a SAR		
Consent	Check process and records in detail to ensure existing consent meets the GDPR standard	May - June 2018	
	Communicate additional information to stakeholders in advance of processing including:		
	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 GDPR		
	Records must be kept of how and why consent given		
Processing children's data	Review and update procedures for processing children's data	May 2018	
	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 criteria of the GDPR- Encryption of laptops, emails etc	September 2018	
Data Breach Response Plan	Review and revise your schools data breach incident response plan	June 2018	
	Mandatory breach reporting within 72 hours		
Data Protection Impact assessment (DPIA)	The school must assess the impact of the envisaged processing operations on the protection of personal data	June 2018	
	DPIAs should 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	Appoint a Data Protection Officer (DPO) to	May – June 2018	
	Advise and inform the school and its staff about their obligations to comply with GDPR and any other data protection legislation		
	Monitor the school's compliance to GDPR		
	Be the first point of contact to the ICO and data subjects		
Processing Agreements	Review and if necessary renegotiate agreements which involve the processing of personal data	May – June 2018	
Policies and procedures	Draft policies to comply with GDPR	May – June 2018	