GDPR Readiness Tracker

1: Accountability and governance	None	Part	Most	Done	Notes
1.1: Awareness					
1. The senior leadership team is aware that data protection laws are changing to the GDPR and appreciate its impact in school.					
2. Your school has identified areas that may cause compliance problems under the GDPR and has recorded these on the school's risk register.					
3. Your school has raised awareness across all areas in school where personal data is handled that changes are coming.					
4. Resources and funding have been assigned for this major change in data protection.					
1.2: Accountability					
1. Your school has identified a management structure, support and direction for data protection compliance within a framework of policies and procedures.					
2. Your school monitors compliance with regular reviews which include the effectiveness of data handling, processing activities and security controls.					
3. Your school has developed and implemented a data protection training programme for all staff, which will include teachers, administration staff, caterers, ground staff, governors, etc					
1.3: Information you hold					
1. Your school has documented:					
a. what personal data is held, student and adult					
b. where that data came from					
c. who it is shared with					
2. Your school has planned to conduct an information audit to map data flows.					
3. Your school has carried out an information audit to map data flows.					

GDPR Readiness Tracker

1: Accountability and governance - continued	None	Part	Most	Done	Notes
1.4: Data Protection by Design and Data Protection Impact Assessments					
1. Your school has implemented appropriate technical and organisational measures to demonstrate it has considered and integrated data protection into processing activities.					
2. Your school understands a data protection impact assessment (DPIA) must be carried out and has processes in place to action this. A DPIA's purpose is to "evaluate the origin, nature, particularity and severity" of the "risk to the rights and freedoms of subjects" before processing personally identifiable information.					
3. Your school has a DPIA framework which links to its existing risk management and project management processes. The DPIA "should include the measures, safeguards and mechanisms envisaged for mitigating" the identified risks.					
1.5: Data Protection Officers					
1. Your school has appointed a Data Protection Officer (DPO). The GDPR does not specify the relevant qualifications that DPOs need, but it does require a DPO to have "expert knowledge of data protection law and practices."					
2. Your school supports the DPO through provision of appropriate training and reporting mechanisms to senior management.					

GDPR Readiness Tracker

2: Key areas to consider	None	Part	Most	Done	Notes
2.1: Lawful basis for processing personal data					
1. Your school has reviewed the various types of processing carried out.					
2. You have identified the lawful basis for all processing activities and this is documented. 6.1					
3. Your school has explained the lawful basis for processing personal data in its privacy notice(s) and through other communication. This will include data sharing policies with 3rd parties including systems such as messaging, payments, cashless catering, etc					
2.2: Consent					
1. Your school has reviewed how it seeks, records and manages consent.					
2. Your school has reviewed the systems currently used to record consent and implemented appropriate mechanisms to ensure an effective audit trail.					
2.3: Children					
1. Where services are directly used by children, you communicate privacy information in a clear plain way that a child will understand.					
2. When required, your school obtains parental or guardian consent.					

GDPR Readiness Tracker

3: Individuals' rights	None	Part	Most	Done	Notes
3.1: Communicating privacy information					
1. Your school has reviewed its current privacy notices and has a plan in place to make any necessary changes in time for GDPR implementation.					
3.2: Individuals' rights					
1. Your school has checked procedures to ensure that it can deliver the rights of individuals or parents under the GDPR.					
3.3: Subject access					
1. Your school has reviewed procedures and has plans in place for how it will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR.					
2. Your school has reviewed procedures and has plans in place for how it will provide any additional information to regulatory bodies as required under the GDPR.					
4: Breach notification	**None**	**Part**	**Most**	**Done**	**Notes**
4.1: Data breaches					
1. Your school has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively.					
2. Your school has mechanisms in place to assess and then report relevant breaches to the ICO within 72 hours where the individual is likely to suffer some form of damage, in particular to identity theft or confidentiality breach.					
3. Your school has mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.					
5: Transfer of data	**None**	**Part**	**Most**	**Done**	**Notes**
5.1: International					
1. If your school operates outside the UK, it has determined the school's lead supervisory authority and documented this.					