Compliance Activity Checklist

1. Basic Evidence Pack			Statutory	Best Practice	Task Completed
A	Roles:	A Data Protection Officer is in place with a documented role description (if internal)/ Contract (if external)	✓		□
		A Risk Owner is in place with a documented role description		✓	□
		A Point of Contact Person is in place to manage an external DPO relationship, with a documented role		✓	□
		A group which makes decisions on Data Protection issues has their remit documented in their Terms of Reference		✓	□
B	Assets & Flows:	Complete an Information Asset Register	✓		□
		Complete a Data Flow Register	✓		□
C	Security:	Review the 'Technical Security' section of the Security Measures document with your IT Support and amend as necessary following a) understanding how your IT Security currently works, and b) any improvements you agree based on risks you've identified	✓		□
		Review the 'Organisational Security' section of the Security Measures document and amend as necessary	✓		□
D	Retention:	Review the Retention Schedule amending any rules where you wish to do so		✓	□
		Record decisions over why you have decided to change any retention rules		✓	□
E	Privacy Notices:	Identify which Privacy Notices are relevant to you	✓		□
		Review each relevant Notice and amend any 'red font' content	✓		□

		Create a website page and publish the Privacy Statement including links to the relevant Privacy Notices	✓		□
		Review the forms you use to obtain data ensuring you provide links to the right Privacy Notice for the type of data you're asking for.	✓		□
F	**Policies:**	Review the template policies and if you intend to adopt them 'as-is', ensure that you can fulfil the commitments being made	✓		□
		Make any additions you identify as a result of decisions over any new rules or clarifications you wish to introduce		✓	□
		Make policies available to employees through your normal policy awareness processes	✓		□
		Publish the Data Protection and Statutory Requests policies on the website in the same location as your other policies		✓	□
G	**Suppliers:**	Identify your Data Processors	✓		□
		Establish an evidence file containing the 'Controls' you have over your Processors (contract/ agreement/ Terms & conditions, their Privacy Policy etc)	✓		□
		Review these Controls to decide whether they are sufficient	✓		□
		Contact Processors for whom you have insufficient evidence asking for additional assurances	✓		□
		File assurance responses on the evidence file	✓		□
H	**ICO Register:**	Check the ICO's Register of Data Controllers (ICO website) to confirm that you have a current entry, taking note of the expiry date	✓		□
		Create a register entry if there is none	✓		□
I	**Awareness:**	Brief employees on GDPR changes	✓		□

		Make information available to parents to raise awareness over their rights		✓	□

2. Activity Management					
A	**Impact Assessment:**	Adopt a method for conducting Data Protection Impact Assessments consistently	✓		□
		Identify (on your Information Asset Register) the assets which will require assessments if there is a change to way you manage the data in the future		✓	□
		Identify the individual who will conduct Data Protection Impact Assessments and liaise with the DPO over approval	✓		□
		Make sure that employees who have the authority to buy software or engage suppliers are aware of the need to consult the individual who conducts impact assessments		✓	□
B	**Security Incidents:**	Adopt a process for managing security incidents	✓		□
		Ensure that the definition of a security incident is known to employees	✓		□
		Identify the individual to whom staff should report security incidents		✓	□
		Identify the individual who will record incident investigations		✓	□
		Identify a means of reporting incidents when the school is not open		✓	□
		Identify the individual who will contact the DPO for advice on notifying the ICO		✓	□
		Identify the individual who will approve any decision to notify the ICO following receipt of DPO advice	✓		□

C	**Procurement:**	Identify the individual who will ensure that Data Protection procurement risks are identified and decide (with advice from the DPO) on the appropriate ‘controls’ over the supplier	✓		□
		Ensure that employees authorised to buy systems and services involving personal data are aware of who to consult over ensuring appropriate ‘controls’ are in place		✓	□
D	**Sharing:**	Use the Records of Processing Activity (ROPA) spreadsheet, Data Flow Mapping (DFM) tab to identify who the School shares data with	✓		□
		Use the ROPA spreadsheet to identify why you are allowed to share data in this way (identifying the legal conditions and any sharing agreements)	✓		□
		Use the ROPA spreadsheet to explain how data should be shared securely	✓		□
		Ensure the bodies you share data with are described on Privacy Notices	✓		□
		Ensure there is a process for getting the advice of the DPO whenever there is a request to share data with a body not already captured on the ROPA record	✓		□
E	**Non-Disclosure:**	Identify any individuals who the school allows access to personal data, who aren’t employed by the school or by a contractor (e.g. Volunteers)	✓		□
		Ensure these individuals sign Non-Disclosure Agreements and that these records are kept in line with your retention periods for staff	✓		□
		Ensure that the process for approving such individuals to work in the school in the future requires an ‘NDA’ to be signed and retained	✓		□
F	**Rights:**	Ensure staff are aware of how to recognise requests and complaints under GDPR rights and direct the request to an individual responsible for co-ordinating with the DPO		✓	□
		Ensure that there is a process to record requests, and to send them to the DPO as soon as possible		✓	□
		Ensure that there is a clear process to approve suggested responses from the DPO, to respond and to log	✓		□

3. Review					
A	Reporting:	Decide on what GDPR performance data you wish to report to the appropriate decision-making body within your existing annual reporting process. (This will capture some elements of the requirements below)		✓	□
		Ensure that those responsible for recording this information are aware of the reporting requirements and when the data will be required		✓	□
B	Policy:	Ensure that a process is in place for an annual review, amendment and approval of policies which are relevant to GDPR compliance.		✓	□
		Record this process on a Policy Change log		✓	□
C	Risk:	Undertake an annual review of your personal data risks as recorded on your Risk Register		✓	□
D	Contracts:	Undertake an annual review of Data Processors to ensure the services are being delivered in a compliant manner and that there is sufficient documentation in place to explain how the service is delivered		✓	□
E	Training:	Undertake an annual review of the effectiveness of information governance training, using staff feedback and analysing the nature and frequency of security incidents		✓	□
F	CCTV:	IF APPLICABLE ONLY: Undertake an annual review of CCTV cameras and use the CCTV register to assess and confirm whether you are satisfied that the continued use of CCTV is necessary	✓		□
G	ICO Register:	Ensure the content of your registration with the ICO has been reviewed as part of the process for making the required ICO annual payment	✓		□
H	DPO:	Provide evidence of these activities (3A-G above) to the DPO ahead of reporting to the Governing body		✓	□
		Include the DPO’s response commentary within the annual report to the Governing Body	✓		□
		Minute the Governing Body’s consideration of the report and any resulting actions		✓	□