Ref	Theme / Question	IG guidance notes	Response
1	**Information Governance/Data Protection Officer (DPO)**		
1a	Have you published the DPO details as part of your privacy notices?	Privacy Notices should include details of your DPO and how they can be contacted: Stockport Metropolitan Borough Council 1st Floor Stopford House Stockport SK1 3XE dpa.officer@stockport.gov.uk 0161 474 2227	Yes
1b	Have you registered with the Information Commissioner's Office and paid your data protection fee?	All organisations which process personal data must be registered with the ICO and pay a data protection fee. https://ico.org.uk/registration/new If you are unsure if you are registered please find your school on the following link: https://ico.org.uk/ESDWebPages/Search	Yes
1c	Do you provide governors with assurances about your data protection practices?	Governors and Trustees are ultimately responsible for data protection and should be kept informed of any breaches/information risks. This may be through meetings or reports.	Yes
2	**Policies**		
2a	Do you have an up-to-date Data Protection Policy in place?	Please see supporting documents on SLA Online for a template Data Protection Policy (V5) and ensure this is published on the school website.	Yes
2b	Do you have policies in place to manage individual rights, eg, data subject access, erasure, rectification, etc?	Please see supporting documents on SLA Online for a template Individual Rights Policy (V5) and ensure this is published on the school website.	Yes
2c	Do you have breach management and information security policies?	Please see supporting documents on SLA Online for Data Breach Policy (V5).	Yes
2d	Do you have records retention policies or guidelines in place?	Please see supporting documents on SLA Online for our Records Retention Schedule (V5). This is for internal use.	Yes
3	**Privacy notices (fair processing)**		

3a	Do you have Data Protection Act 2018 & UK GDPR compliant Privacy Notices in place?	*Please see supporting documents on SLA Online for template Privacy Notices (V5) on the following:* *Pupils* *Workforce* *Visitors* *Governors* *SEN and Safeguarding* *These should be published on the school website.*	Yes
3b	If your organisation has CCTV on site does this have visible signage and has a CCTV policy been compiled?	*Please see supporting documents on SLA Online for CCTV policy (V5). This will not apply to you if you do not use CCTV.*	Yes
4	**Records of Processing Activities (RoPA)**		
4a	Do you have a RoPA in accordance with the accountability principle?	The Record of Processing Activitites (ROPA) is a document detailing information processed by the organisation and includes who is responsible for it, where it is stored and how it is kept secure. A Personal Data Audit (PDA) needs to be completed which will then form your Record of Processing Activities.	Yes
5	**Training and awareness**		
5a	Have all staff received data protection training or been made aware of the Data Protection legislation?	Online Mandatory Data Protection Training is available for all staff and should be completed on an annual basis. Please ask the Information Governance Team for more details. Annual advanced training is available to Headteachers and School Business Managers from the IG Team.	Yes
5b	Is Data Protection training included in staff induction?	Online Mandatory Data Protection Training is available for all staff. Please ask the Information Governance Team for more details.	No
5c	Do you regularly communicate with staff about data protection good practice?	This may be through staff communication or via staff meetings	Yes
6	**Suppliers**		
6a	Do you have contracts in place with suppliers/data processors (those processing personal data on your behalf)?	Contracts need to be in place with other companies that provide software to the school or have access to any personal data to ensure the organisataion's data is processed legally.	Yes
6b	Have you reviewed these contracts and/or contract templates to check they are compliant with data protection legislation	Processing contracts should contain at least standard DP clauses. These are listed by the ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/	No

6c	Do you perform due diligence when procuring new software to ensure the data processor is data protection compliant?	Checks should be made when purchasing new software that the organisation is data protection complaint.	
7	**Individual rights**		
7a	Do you log requests in relation to individual rights, eg access, rectification, erasure, objection etc?	Individual Rights Requests should be logged on a secure system. (If you have not had any requests please state this in the comment box.)	Yes
7b	Did you answer requests within the statutory timescale?	Individual Rights Requests should be logged on a secure system.	Yes
7c	Have you received any complaints from individuals or the ICO in relation to data protection rights?		No
8	**Breach handling**		
8a	Do you log data protection breaches eg, security, records management, theft, losses, near misses?	Once you report a data breach to the Information Governance Team we log the incident on our system. However, the school should keep a log too as the Data Controller.	Yes
8b	Where necessary, did you tell the individuals concerned about the breaches?	This is dependant on how high the risk is and is determined on the advice Information Governance provide.	Not applicable
8c	Did you report breaches/Incidents to the Information Governance Team within 24 hours of being informed?	All breaches must be reported to the IG team within 24 hours of being informed of the breach. Please select not applicable if you have ahd no breaches in the last year.	Not applicable
8d	Did you take remedial actions to reduce the risk of recurrence and record these actions on a risk register or equivalent?	Organisations should try to reduce the risk once they become aware of a breach/incident and record and implement any actions recommended by the DPO.	Not applicable
8e	Have you received any complaints from individuals or the ICO in relation to data protection breaches?		Not Applicable
9	**Requests for personal information disclosure**		
9a	Do you request individuals provide identification when fulfilling requests for personal information?	An organisation should ensure it is only providing data to the correct individual. This does not apply if the requester is know to the school ie current student/parent.	Yes

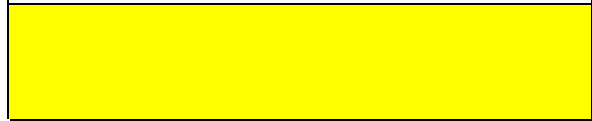|			
9b	Do you ask for requests to be made in writing, eg, from police, other parties?	A Police Schedule 2 (819b) form is available to use on SLA Online if the police ask for information.	Yes
9c	Do the requests cite the data protection lawful basis ie, legal reason for disclosure?	An organisation should be satisfied it has a legal reason for disclosure under data protection legislation	Yes
9d	Do you log disclosures of personal data to provide an audit trail for your records?		Yes
10	**Records management**		
10a	Do you operate a confidential waste system for personal data?	Information in paper format should be destroyed securely when no longer needed.	Yes
10b	Are your paper record repositories secure/access controlled?	Information should be viewed on a 'need-to-know basis' only and paper kept securely.	Yes
10c	Do you maintain a list of records which have been destroyed and who authorised the destruction?	This can be via an electronic audit trail or manual one.	
10d	Do you keep an audit trail to changes in personal data?	This could be via software or processes	Yes
11	**Security**		
11a	Do you use an external company for IT or do you have provision onsite?	Who is responsible for securing your IT network?	External
11b	If internal - Does your IT network have appropriate controls in relation to detection/prevention of intrusion, content monitoring, firewalls etc?		Yes
11c	Do you have business continuity/disaster recovery plan for both physical and IT incidents?		Yes
11d	Do you use encryption and/or pseudonymisation where it is appropriate to do so?		Yes
11e	Do you operate access control based on role?	Information should be viewed on a 'need-to-know basis'. Processes should be in place to restrict viewing to job need and leavers should be removed from software access.	Yes

11f	Do you ensure computers/laptops/removable media has all data cleansed when no longer in use?	All data should be destroyed from electronic equipment before disposal. Many external companies can arrange this or you can use a degausser.	Yes
12	**Freedom of Information**		

Evidence/Comment (please provide evidence i.e. URLs or provide a comment on your response)
All details on privacy notices on website
ICO Registration Number: Z477252X Date of expiry:03.04.2024
Policy in place
Policy in place
Policy in place
Policy in place

Privacy notices in place

Policy in place

PDA completed and passed to IG March 2022 and 2023

Annual Refresher training undertaken by Headteachers and School Business Managers .
Staff will be given data protection training via Learning Pool

This is to be included in thhe new staff handbook and trainiing given via learning pool

When we receive updates these will be communicated to staff

Staff who manage the contracts with data suppliers have been informed of the need for data processor contracts.

NO REQUESTS RECEIVED AS AT 28.03.23
NO REQUESTS RECEIVED AS AT 28.03.24
NO REQUESTS RECEIVED AS AT 28.03.25
NO DATA BREACHES AS OF 28.03.2023
NO DATA BREACHES AS OF 28.03.2024
NO DATA BREACHES AS OF 28.03.2025
NO DATA BREACHES AS OF 28.03.2026
NO DATA BREACHES AS OF 28.03.2027
YES IF REQUIRED

NO REQUESTS MADE TO 28.03.23
NO REQUESTS MADE TO 28.03.24
NO REQUESTS MADE TO 28.03.25

WE USE STE WASTE TO DISPOSE OF CONFIDENTIAL WASTE. ALSO SHREDDER AVAILABLE AT SCHOOL
YES IN LOCKED AREA
VIA SECURE SYSTEMS
ARK TECHNOLOGY
YES PLAN IN PLACE