GDPR CHECK LIST CAMBO FIRST SCHOOL

We are compliant - This audit will be presented to the Governing Body in November 23

Policy on the website. DPO remains in place (PW). Data Controller remains in place [PC]

All staff and parents have received privacy statements.

We are cutting down radically on filing hardcopies and storing information on the cloud using MIS. Hardcopies are seen as a weak point.

A new high powered shredder was purchased to destroy when no longer required. September 23.

Privacy notice updated October 23 has been reviewed and remains unaltered.

Destruction of past information to apply with GDPR that has been stored within school. Aut 23

Admissions information stored digitally. Password protected.

All absence correspondence goes via the school secretary (DP) and is entered onto the MIS system. There are no hardcopies.

Universal safeguarding touched on the importance of protection and what information can be shared.

Email security of a sensitive nature destroyed. Headteacher and secretary use Cryptshare to transfer sensitive information to schools and the LA.

All visit consent forms/risk assessments are shredded.

All policies and proforma are in place and have been ratified by the governing body including

- Digital continuity
- Freedom of information
- GDPR
- Records Management
- Security Breach

All necessary GDPR policies are on the Cambo School Website. Parents/Staff and Governors have also been emailed copies of the GDPR policies.

Training has taken place for senior staff regarding the GDPR via NOS.

Our Freedom of information statement has been uploaded to the website and is included in our prospectus for new parents. Updated annually

Requests for data under the Freedom of information Act and data breaches are fed back to the governing body as and when necessary and GDPR is a standing item within termly governing body meetings.

PAV Walker

Questions	Yes/No	Evidence	Further comments	Data controller	Data processor
General					
Is data handling a fixed item in senior leadership team (SLT) meeting agendas?	Yes	This is linked through to the Governing body e.g. Chair is Data Controller. Standing item on HT report Gov Meetings agendas and minutes. NCC SLA agenda/minutes available for viewing	The data protection officer (DPO) attends all Gov/SLT meetings to ensure data handling is discussed. Standing item on gov body meetings	✔	✔
Is the HT / DC and data processor fully aware of: ● The school's obligations imposed by the GDPR? ● The potential repercussions imposed, should the school fail to comply with the GDPR?	Yes	CPD training has been organised. The DPO is also the DPO for the Church. Agenda, minutes of meetings to discuss evident. Included in	We are a small school. The senior leadership role is limited to the Headteacher. The GDPR DPO is Mrs Pam Walker.		

• The rights provided to individuals by the GDPR?		the full Governor Body meeting Autumn 23 / Summer 24 will remain so in the Headteachers report for future meetings. Policy into practise. GDPR compliant Record Management GDPR Data Protection Policy Privacy Notice Freedom of Information Policy Security Breach Management Plan Digital Continuity Statement GDPR Information for all staff Data sheets re requests	All evidence has been pulled together via PC Headteacher , CF Secretary Policies updated/ ratified by Governors in line with Brexit. June 22/23 1 minor breach linked to bcc Head Teacher sent email to Reception Teacher. In error she clicked on the teachers home email address instead of her school address - The email was sent to a parent. The parent responded to the teacher via her personal email. DPO contacted, email Email recalled discussion with teacher about the breach. Advised	✔	✔

			to change her email address Telephone conversation with parent and email deleted [HT sight impaired via medical procedure] Recorded on data breach form		
Does the school need to maintain an information asset register?	Yes	Created as part of the GDPR process Data Controller to manage	Ratified by Governors	✔	✔
Is the information asset register reviewed regularly to ensure that the processes undertaken by the school are appropriately reflected?	Yes	Annually or as and when necessary Reviewed July 23	Annual meeting with DC HT S to discuss changes necessary. Governing Body ratified. Informed via termly meeting	✔	□
Has a data controller representative been identified or appointed?	Yes	Governors notes Spring 18 Governors Spring 19 Governors Spring 20/23	We are a small school, it is very difficult to identify a data controller who does not have a vested interest in the school. NCC suggested C of G with Headteacher and Secretary acting as processor Agreed	✔	□

			Governors Spring 18 remains in place 23		
Are all staff members aware of who the data controller representative is?	yes	Staff meeting to discuss knowledge, understanding and impact re GDPR lead by DC / HT / S. Staff Governors kept abreast of developments via email	Annual update Aut 23	✔	✔
Do you need to appoint a data protection officer (DPO)? If yes, had a DPO been appointed?	yes		Chair of Governors – DC / Governors and Headteachers /Secretary processors responsibility	✔	✔
Are there procedures in place for formal review of data protection activities within the school by the DPO?	Yes	Agendas, minutes. SIP visit		✔	✔
Policies and procedures					
Are there policies and procedures in place to ensure compliance with the GDPR?	Yes	GDPR compliant Record Management GDPR Data Protection Policy Privacy Notice Freedom of Information Policy	Reviewed / ratified by Governing Body Annually Shared with staff		

		Security Breach Management Plan Digital Continuity Statement GDPR Information for all staff Data sheets re requests		✔	✔
Are these policies and procedures reviewed within appropriate timeframes?	Yes	Reviewed / ratified by Governing Body Annually Shared with staff	n/a	✔	✔
Does the school provide privacy notices when processing individuals' information? If so, what format are these notices in, and when are they updated?	Yes	Microsoft word Annually	We use the ICO model adjusted to accommodate our school updated for 22/23	✔	✔
Where possible, is the data collected directly from the data subjects and is any information they require given to them?	Yes	Data collection sheet – names, address, DOB etc held in SIMS, We buy into NCC SLAs thus data is also held at NCC level e.g. Payroll	Staff, Governors, Parents, Children, professionals in conjunction with the school e.g. third party contract. 3RD party	✔	✔

			contracts have said how they meet GDPR		
Is there a clear procedure for individuals to request any information about themselves?	yes	Policy into practice	Register of requests also kept. 18-19 1 request 19-20 0 requests 20-21 0 requests 21-22-1 request 22-23 - 2 requests	✔	✔
Are there clear documented policies and procedures for all aspects of GDPR compliance?	yes		Ratified in Governor meeting Summer 18 updated 19 updated 20 updated 21 updated 23	✔	✔
Project management					
Are all new projects and initiatives that include processing information reviewed during the planning stage to ensure data is handled correctly?	yes	None as of yet, although policies outline procedures and practices	good practice	✔	✔
Are data protection impact assessments conducted throughout the stages of planning, including during development, testing and delivery?	yes	None as of yet, although policies outline procedures and practices	Good practice pay policy annually to be done for 23-24	✔	✔

Staff training and awareness					
Are staff members made aware of their responsibilities in line with the GDPR?	yes	Meeting agenda and notes Emails sent to staff Information sent to staff	Update as reminder annually. Complete Sept 23	✔	✔
Does induction training for new members of staff include making them aware of their responsibilities in accordance with the GDPR?	yes	One new staff member. All paperwork in place [CS] Policy into practice which dictates procedures also linked to KCSIE 23	Good practice Induction policy staff hand book	✔	✔
Is refresher training undertaken, and how often?		Staff hand book Email on return to school termly Training as and when necessary re SLT/GDP	Autumn term Staff meeting to discuss aspects of GDPR NOS Refresher training 3 yrs. 2023-PC/CF PW- NOS	✔	✔
If a member of staff has a query regarding data handling, do they know who to seek advice from?	yes	Guidance given in the Book Email termly re GDPR All have policies which outline procedures	Autumn term reminder of GDPR annually	✔	✔

Are staff members made aware of unauthorised behaviour and the boundaries of what they can and can't do in relation to the principles of the GDPR?	yes	Guidance given in the Book Email termly re GDPR All have policies which outline procedures	Autumn term reminder of GDPR annually	✔	✔
Are departing staff members reminded that all information pertaining to staff members, pupils, visitors and other persons, remains confidential even after they have left the school?	yes	We have had no staff leave as such. However: Guidance given in THBook Email termly re GDPR All have policies which outline procedrues	Autumn term reminder of GDPR annually No one has left 22-23	✔	✔
Do staff members' contracts outline their data protection responsibilities?		Contracts Completed via NCC and follow guidellnes.	Any new contracts will outline GDPR responsibilities NCC SLA held at source	✔	✔
Lawful grounds for processing					
Is there a lawful ground for processing the personal data for each processing operation?	yes	Policy into practice	Privacy notice Updated	✔	✔
Is the school's process for obtaining consent compliant with the GDPR?	yes	Policy into practice	Privacy notice Updated	✔	✔
Does the school explain processing to its pupils, where relevant, in accordance with the GDPR?	no	Parents, staff, governors and community	Children are very young. We focus on safeguarding of passwords/addresses etc through e-safety	✔	✔

			NOS newsletters sent to parents		
Are data subjects made aware of the data processing for which they can withdraw their consent?	yes	Policy into practice Privacy notice annual	Consent form completed termly For specific events individual consent sought	✔	✔
Transparency requirements					
Are data subjects fully informed of the processing of their data and are they given updates on the status of the processing?	yes	Privacy notice Policy into practice	Where and when necessary – policy into practice Privacy notice updated	✔	✔
Data protection principles and accountability					
Is personal data only used for the purposes for which it was original collected?	yes	Policies into practice	We follow procedures for archiving and shredding data	✔	✔
Is any personal data that has been collected limited to what is necessary for the purposes of processing?	yes	Policies into practice	We follow procedures for archiving and shredding data shredding 23 aut	✔	✔
Are policies and training in place to ensure personal data is checked and, if inaccurate, corrected?	yes	GDPR Training re PW, PC, CF Buy into SLAs at NCC level	no breaches as of yet	✔	✔

Are policies and documents in place that outline the procedures for archiving and destroying data?	yes	Outlined in Policies	We follow procedures for archiving and shredding data Record management policy reviewed Relevant paperwork destroyed via cross shredder Oct 23	✔	✔
Are appropriate security measures in place to protect data?	yes	NCC SLA protection of data Encryption/software via NCC. Website also covered Locked filing cabinets	We follow procedures for archiving and shredding data	✔	✔
Data subject rights					
Is there a procedure for handling, accepting and processing subject access requests (SARs)?	yes	Policy into practice	Excel document for recording access requests.	✔	✔
Does the school offer a straightforward process for individuals to access information held about them?	yes	Policy into practice	Excel document for recording access requests.	✔	✔
Does the school process SARs within one month (or longer under exceptional circumstances), in accordance with the GDPR?	yes	Policy into practice	Excel document for recording access requests.	✔	✔
Does the school provide data in a commonly used, clear and accessible format?	yes	Policy into practice	Excel document for recording access requests.	✔	✔

Are individuals informed of their right to demand that data pertaining to them is destroyed or amended?	yes	Privacy notice Policy into practice	Excel document for recording access requests.	✔	✔
Are controls in place to allow personal data to be erased or blocked?	yes	Policy into practice Policy Central SIMS SLAs re most information held at NCC level 3rd party contracts show how data will be protected	We follow procedures for archiving and shredding data	✔	✔
Can the school's current procedures effectively manage requests such as erasing and blocking?	yes	Policy into practice Policy Central SIMS SLAs re most information held at NCC level 3rd party contracts show how data will be protected	We follow procedures for archiving and shredding data	✔	✔
Does the school make it clear that individuals can object to certain types of data processing?	yes	Policy into practice all Privacy notice	policies available to all in school. Privacy notice on website and in prospectus. Copy also illustrated in information showcase.	✔	✔

Are policies and procedures in place to ensure rights can be implemented in practice?	yes	Policy into practice all Privacy notice	policies available to all in school. Privacy notice on website and in prospectus. Copy also illustrated in information showcase.	✔	✔
Data security					
Are the risks inherent in processing formally evaluated, tested and assessed, and have measures to mitigate those risks and ensure the security of the processing been implemented?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirments in a written form		✔	✔
Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form		✔	✔
Is there a documented process for resolving security-related complaints and issues?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form		✔	✔

Are industry-standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form		✔	✔
Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained or to fulfil the purpose(s) for which it was collected?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Where and when necessary	✔	✔
Are pseudonyms put in place to protect personal data where possible?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Where and when necessary	✔	✔
Can the availability and access to personal data be restored in a timely manner in the event of a physical or technical incident?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Data backed up weekly data storage back up kept in safe	✔	✔
Data breaches					

Does the school have a documented privacy and security incident response plan and incident identification system?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Data backed up weekly data storage back up kept in safe Completed via CF	✔	✔
Are the plans and procedures regularly reviewed and tested?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Data backed up weekly data storage back up kept in safe	✔	✔
Are there procedures in place to notify the relevant authority, e.g. ICO, and data subjects of a data breach, where applicable and within the 72 hour timeframe?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔
Is there clear internal guidance explaining when notification of a breach is required and what information needs to be reported?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔

Are there clear procedures in place to notify the controller in the prescribed form of any data breach without undue delay after becoming aware of it?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔
Are data breaches documented?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions. Specific excel document to record breaches and actions etc.	✔	✔
Are there cooperation procedures in place between processors, suppliers and other partners to deal with data breaches?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔
Has the school considered data breach insurance cover? (not mandatory under the GDPR)	no	We just couldn't afford it. But in buying into third party there is a legal obligation re data breaches		✔	✔
International data transfers					
Is any personal data that is transferred outside the European economic area done so in compliance with the GDPR?	yes	Policy into practice outlines all procedures	Policy outlines all areas and actions	✔	✔

		3rd Party contractors have shown how they will meet GDPR requirements in a written form			
When data is transferred, what is the purpose of the transfer, and is it clear who the recipient is?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔
Are details of all transfers listed, e.g. the nature of the data and purpose of the transfer?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔
Is the legal transfer adequacy mechanism for each transfer identified and listed?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔
Are specific transfers appropriately covered by an implemented adequacy mechanism or by an exception?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet	Policy outlines all areas and actions	✔	✔

		GDPR requirements in a written form			
Are data subjects told of any intended transfers of their personal data?	yes	Policy into practice outlines all procedures 3rd Party contractors have shown how they will meet GDPR requirements in a written form	Policy outlines all areas and actions	✔	✔
Other controller obligations					
What privacy training programmes does the data controller provide for employees?	yes	PC/CF NCC training 2018/23 ICO support on website update as and when required. Any other training as and when required	Policy outlines areas and actions	✔	
Do you operate a regular audit review process?	yes	annually	GDP/Governor visit annually reporting to governors termly via HT report	✔	
Do policies and procedures build in a requirement to integrate compliance into processing activities?	yes	Policy into practice	Policy outlines areas and actions	✔	
Has a DPO been appointed, where necessary?	yes	Chair of Governors HT/SB – processors	Policy outlines areas and actions	✔	
Where a DPO is appointed, are escalation and reporting lines in place?	yes	Chair of Governors	Policy outlines areas and actions	✔	

		HT/SB – processors			
Is sensitive personal data processed?	yes	Sims/NCC/SLAs	Policy outlines areas and actions	✔	
Are the legal grounds for processing personal data recorded?	yes	Chair of Governors HT/SB – processors	Policy outlines areas and actions	✔	
Do you have a process for identifying the need for and conducting (and documenting) DPIAs?	yes	Chair of Governors HT/SB – processors	Policy outlines areas and actions	✔	
Do you undertake and record prior diligence of service providers?	yes	Chair of Governors HT/SB – processors	Policy outlines areas and actions	✔	
Are there controller/processor contracts containing all the stipulated terms?	no	Unpaid roles	Description of roles outlined	✔	
Other processor obligations					
Are there controller/processor contracts in place containing the stipulated terms?	no	Unpaid roles	Description of roles outlined		✔
Are the legal grounds for processing personal data recorded?	yes	Policy into practice	Procedures followed		✔
Where a DPO is appointed are escalation and reporting lines in place?	yes	Policy into practice	Procedures followed		✔

Are you able to assist the data controller in ensuring compliance under the GDPR?	yes	Policy into practice	Procedures followed		✔