

Annual GDPR report

LITTLE HAYES NURSERY SCHOOL

Table of contents






4C-IT in partnership with HelpmeHelpme Ltd was engaged to conduct the GDPR Compliance Assessment for <School name>















Introduction



This assessment report details the high level information required to show GDPR compliance, along with the controls that have been put in place to protect all data and its usage. The information collections are categorised using the following criteria: -

Type	Description
Personal	Personal data that is used to identify individuals. This includes all personal details including contact details and any level of personal detail the school is required to retain
Financial	Financial data that is used by the organisation for both internal and external utilisation.
Supplier	Supplier data that is used for management of suppliers, this can sometimes include personal data and is therefore required to be protected.

Information Collection Assessment










	Requirements	Information	Assessment	Status
1		Raise GDPR Awareness GDPR awareness presentation, detailing the changes to legislation and your responsibilities	GDPR Awareness presentation to all key stakeholders and all members of staff has been completed.	
2		Know your information Carry out an information collection audit using the record of processing	All information collections are ongoing and are being identified.	
3		Privacy communications Review of privacy statement and Data Protection Policy. Creation of template Privacy statement to use for all your communications - internet, email, marketing and contractual communications. This privacy statement is to be written in plain language and not "legal speak"	The Privacy Statements for all situations have been created and published to our website. Links within all correspondence to the Privacy statement have been implemented	

	Requirements	Information	Assessment	Status
4		Individual Rights Ensuring processes are updated to reflect how you delete individual's information within the remit of all legislation. Review how information is provided to individuals in a common format	The Privacy Statement for all situations have and published to our website. Links within all correspondence to the Privacy statement have been implemented	
5		Subject Access Request (SARs) Implement a plan for handling SARs and providing required information within the 40day notice period. Communicate the parameters of SARs	A Subject Access Request Policy is required to be created and implemented	
6		Be legal Understanding the different types of data processing your organisation performs. Identify the legal basis for carrying out such tasks and document each separately	The majority of information collections have been identified and the type of data being held assigned within the Information Collection questionnaire. The types of data are detailed within the flow charts for each information collection.	
7		Consent How you seek, obtain and determine consent for individual's data to be used and/or shared	For each information collection a determination has been made on whether formal consent is required to be asked for. Where consent for an individual's information is to be shared outside our organisation this has been requested.	
8		Protecting children's data Using the schools MIS system to update records and to seek consent from a guardian for a data processing activity relating to a child	The school have determined that the processing and control of children's data/information is an integral part of our operations	
9		Data breaches Implement process for detecting, investigating and reporting data breaches to customers and regulatory body	The School do not have in place a Security Incident Management Policy	
10		Privacy by Design Privacy impact assessment (PIA) to be detailed within the GDPR assessment report about the risk assessment of all information collections identified in 2. Know your Information	The majority of impact assessments as well as a risk assessment has been conducted on all identified information collections.	
11		Data Protection Officer (DPO) Assign a DPO if your organisation processes large scale data and information as part of your main	The School have assigned a Data Protection Officer.	

	Requirements	Information	Assessment	Status
		operations. It is your decision on whether you require a DPO or not		
12		International? Within 2. Know your Information ascertain if any data is held or processed internationally. Any data held or processed outside the UK/EU is required to be identified and detailed within your privacy statement	The School hold, process and manage the information collections used for our operations outside of the UK/EU geographical area. The Privacy Statement reflects where information is held and managed.	

Policies and Processes

The following documentation and activities have been implemented to, not only show compliance to the regulations but also, to implement “industry best practice” for the protection of information and IT infrastructure.

Document	Status
Privacy Statement	
Data Protection Policy	
Backup Policy	
Malware / Anti Virus Protection Policy	
Encryption Policy	
Subject Access Request Policy	
Data Removal Request Policy	
Security Incident Management Policy	
Information Audit Policy	

Conclusion

The School have completed the GDPR Compliance exercise and are implementing all necessary controls and protections for all information collections. The recommended treatment plan from the initial report has been partially implemented within our organisation due to financial and resource constraints but has a whole the school have implemented as much as they can.

All personnel have received GDPR awareness training and addition training will be given annually.

While not all implemented documents and activities have been completed the process is ongoing are to be reviewed on an annual basis, as per our Internal Audit Process. Over the next few months’ school should have completed all the required processes and will be compliant as to the best of their ability as GDPR is an ongoing project.