

Ellingham CofE Primary School GDPR Compliance Visit – 2023-24

Purpose of Visit: To ensure the school is compliant with the GDPR and demonstrating best practise whilst dealing with any personal data. Please note this template is not exhaustive and should not be your sole method for ensuring compliance.

ITEMS FOR CONSIDERATION	DISCUSSION POINTS	Notes
Data Breaches	<p>Has the school had any data breaches? If so, could they have been avoided? Was the breach procedure followed?</p> <p>Resources available: Data Breach Flow Chart. 5 minute GDPR refresher slides that can be added to any in house staff training.</p>	None
Subject Access Requests	<p>Has the school had any SARs? If so, were there any complexities or concerns when replying to the SAR?</p> <p>Resources available: SAR Flow Chart. 5 minute GDPR refresher slides that can be added to any in house staff training. ICO Model Publication Scheme and Schools Guide to Information briefing note/documents. Support from DPO with this</p>	One SAR – information was shared. No DPO advice needed.
Staff Training	<p>Has training been provided to the staff to ensure they know how to comply with GDPR day to day? Does induction training for new staff include a section on GDPR?</p> <p>Resources available: GDPRiS Posters. 5 minute GDPR refresher slides that can be added to any in house staff training. Full staff training from DPO.</p>	Training has not been done for some time. DPO will circulate GDPR training slides for staff to complete at the next teacher training day.
Retention of Personal Data	<p>Has the school adopted the Records Management Schedule? Any support needed from the DPO?</p> <p>Resource available: NCC Records Management Schedule if not yet in use.</p>	Yes
Destruction of Personal Data	<p>How do you destroy personal data? Could personal data easily be located and erased at request?</p> <p>Primary- retain whilst the child is at the school.</p>	Shredded in-house or incinerated.

	<p>Secondary- Date of birth + 25 years. Resource available: NCC Records Management Schedule</p>	
ICO Registration	<p>Is the school registered with the ICO? Resource available: https://ico.org.uk/for-organisations/data-protection-fee/ and https://ico.org.uk/ESDWebPages/Search</p>	Yes
Policies and Procedures	<p>Are all new projects, systems and initiatives reviewed during the planning stage to ensure data is handled correctly? Is the GDPR management tool updated accordingly to make sure the schools privacy notices are also up to date? Any updates needed now? Resource available: GDPR Management Tool</p>	The Headteacher reviewed all projects, systems, and initiatives on the school's School360 asset list. All areas are now up to date.
Electronic Devices	<p>Are memory sticks still in use? Are chrome books or laptops being used instead for better encryption? Emails- are all staff and governors using a secure email account? Even better a school email for governors?</p>	<p>Some staff use encrypted memory sticks, but mostly Google Drive. The DPO recommended phasing out memory sticks. All laptops and devices are encrypted, and all staff and governors have a secure email account (staff school emails, governors School360 emails).</p>
Website Compliance	<p>Are privacy notices and audit reports published on the schools website? Social media posts are uploaded with consideration of the GDPR? Resource available: adding a pinned post to the top of a facebook or twitter page along the lines of 'Our school ** page has strict Safeguarding rules which we must adhere to if we wish to continue running the page. One of these rules is that we will never post the name of a pupil as this is an open forum that anyone can view. By posting their name, this poses a Safeguarding risk to your child. We respectfully ask parents to not identify their child by name in anything they may comment on. Sadly, if a child is identified by name, we will have no alternative than to remove the whole post. Thank you for your cooperation. We will always be fully committed to keeping your child safe in school and online.'</p>	An annual full GDPR website/social media compliance check is completed by the school's DPO in the Spring term.

<p>Environment Audit</p>	<p>Consider:</p> <ul style="list-style-type: none"> ● Data on walls in classrooms, corridors and offices ● Lockable storage ● Information around the teachers area- desk, computer, notice board etc ● Tracking, SEND, healthcare folders/sheets ● Kitchen and communal areas such as library, intervention spaces and play spaces clear of data 	<ul style="list-style-type: none"> ● Data on walls / classroom displays in classrooms are PII compliant. ● No data in communal areas. ● Paper records are stored in lockable storage in the school office. ● Most teacher spaces PII compliant. Computers locked when not in use. ● One instance of classroom list in teacher's workspace with full names and class group – minor PII risk. DPO recommends first names only for any paper-based class lists. ● Allergy information in kitchen is securely stored away with access available only to leaders and kitchen staff.
<p>Any questions/comments/recommendations</p>	<p>The school is mostly GDPR compliant, with only a few recommendations. The DPO is satisfied that the school has effective GDPR practices in place and has no concerns.</p> <p>The DPO recommends that staff GDPR refresher training be completed at the next training day, the school phases out the use of memory sticks, and that any paper class lists only have first names.</p>	