**GDPR document checklist: what do schools need?**

On 25 May 2018, the General Data Protection Regulation (GDPR) will come into force, meaning the way in which schools store, process and manage data and information will change. In order to ensure that schools are compliant with the GDPR, there are a number of existing documents, such as policies, that will need to be amended to reflect new requirements, as well as entirely new documents that will need creating.

Schools can use this template to check which documents are required, view important information relating to each document and the criteria that needs to be included, to ensure they are compliant with the GDPR ahead of May 2018. Use the relevant column to indicate whether you have the document in place and outline any other comments in the corresponding column, such as further action required.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document title** | **What do I need to know?** | **What needs to be included?** | **In place? (Y/N)** | **Comments** |
| **Data protection impact assessment (DPIA) template** | * DPIAs are needed to identify and reduce the privacy risks of projects, such as installing a new IT system for storing and accessing personal data. * DPIAs can identify the risks of harm to individuals’ rights through misuse of their personal information. * DPIAs can be used to inform the information asset register. | * The aim of the project * Which data will be collected * How the data will be collected * Where the data will be stored * How the data will be shared * How the data will be amended or deleted * Any identified risks to individuals, compliance or the school * Solutions to identified risks * A signature of the individual completing the DPIA * Contact information of the individual for future privacy concerns | No | We need to research this area further in order to complete it. |
| **Information asset register** | * Information asset registers are needed to identify which data a school holds. * It is essential to record whether a school has a legal, statutory or another valid reason to process the data. | * The asset title * Whether it is a key asset * The activity status (ceased, ongoing, future) * The purpose description * Whether it is personal data and also if it is sensitive personal data * Whether consent has been sought and meets the requirements of the GDPR * Sensitive processing conditions and the need for sensitive processing * Legal processing conditions and the need for legal processing * The name of the information asset owner * Whether it is a public domain * The published location * Who the data will be shared with and accessed by * General description of the risks involved * General description of the security measures in place to protect the data * Time limits for processing the data * Retention of the data * The type of disposal required and the disposal method, as well as the date of disposal | No |  |
| **Privacy notice** | * Privacy notices are required to outline to the school workforce, pupils and their families how the school holds their data. * Privacy notices must be written in a way that makes it suitable for the intended audience. * Schools should outline the legal, statutory or other requirement for processing the personal data. | * The identity and contact details of the data controller and data protection officer (DPO), where applicable * The purposes of processing the data, as well as the legal basis for processing, including the legitimate interests pursued by the controller * The recipients or categories of recipients of the personal data, if any * If transferring data, the fact that the controller intends to do this and how it will be transferred * The retention period of the data (or, if that is not possible, the criteria used to determine that period) * The right to request access or amendments to, and erasure of, the data, or restrict the processing * Where the processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal * The right to submit a complaint to the Information Commissioner’s Office (ICO) * Whether the data is statutory or contractual data, and whether the subject is required to provide the data and the consequences of not doing so * Any consequences, or risks to the data subject, of processing the data * The existence of automated decision-making | Yes  Yes  Yes |  |
| **Consent form** | * Consent forms are required to demonstrate that data subjects gave their consent to processing their personal data, where applicable. * Schools must be able to demonstrate that consent was freely given. * It must be clear how data subjects can withdraw their consent. | * The specific purpose for which the data is being processed – it must only be processed for this purpose * The retention period of the data in order to fulfill the purpose for which it is being processed * The terms and conditions for consent – written clearly and concisely * The right for individuals to withdraw consent at any time, and an explanation of how to do so * Any other information that is necessary to process the data | Yes |  |
| **Subject access request information** | * Schools are required to inform individuals of their rights to access the data that the school holds about them. * Individuals should be informed of how requests will be handled. * If a request is refused, the school must tell the individual the reasons for this, and inform them of their right to complain to the ICO. * Requests must be responded to within one month. | * A summary of data subjects’ rights to access their data, which includes the right to: * Be informed of the personal data the school holds about them. * Access their personal information. * Have their personal information rectified or erased. * Restrict processing of their data. * Object to the processing of their data. * Data portability, to obtain and reuse their personal data for different purposes (and the circumstances in which this applies). * Not be subject to automated decision-making, including profiling. * The process for submitting subject access requests * The responsibility of the school to respond to subject access requests * That requests are free of charge in most cases, other than the right of the school to refuse or charge for requests that are manifestly unfounded or excessive | Yes |  |
| **DPO role descriptor** | * All public authorities or establishments which carry out large-scale, systematic monitoring of individuals must appoint a DPO. * The DPO is responsible for overseeing and monitoring the school’s data processing practices, and ensuring compliance with the GDPR. | * The core responsibilities of the DPO relevant to the following areas: * General responsibilities * School procedures * Supporting other members of the school community * Working closely with the controller and processor * The school’s responsibilities, as an employer, to the DPO | No | New role learning as we go along.  We would benefit from a job description. |
| **Data breach record** | * Where a security breach occurs, schools need to record the details of this. * Schools should decide which information is necessary to record suitable to their requirements. | * Date and time of the breach * Outline of the breach – when, what, who, etc. * Whether the breach was conducted by a staff member, their details if so, as well as the last date of any data protection training they received * Type and amount of personal data * Action taken by recipient when they received the information * Action taken to retrieve information and respond to the breach * Procedures in place to minimise risks to the security of data * Details of notification to the affected data subject and whether a complaint has been received * Procedural changes to reduce risks of future data loss * Conclusion – serious/minor breach, likelihood of reoccurrence | Yes | We know what is required but need to establish a file with relevant templates and procedures to follow. |
| **Data protection and security policies** | * Schools must implement policies to address the data protection principles. * Schools may decide to have overarching policies which address all or most of the data protection principles or individual policies. | * Policies which include procedures on the following: * Data protection * Subject access request rights * Data retention * Data security breaches * Processing data * Privacy notices | No | We have a GDPR policy which includes these, but we need to establish a photograph and videos at school policy and a cloud computing policy. We also need to establish privacy notices. |