****

**JMB Support Note accompanying the**

**JMB Template Data Protection Policy**

**Contents:**

**Part One: Action points for customising the template**

**Part Two: Policy Review Activities**

**Part Three: GDPR Training Dates Autumn 2019**

**April 2019**

**Part One: Action Items**

|  |
| --- |
| **Customising the template to reflect your school’s activities** |
| One of the GDPR principles states that personal data must be processed *lawfully, fairly and in a transparent manner*.  Your school’s policy requires that you  i) set out and identify the information that must be communicated to data subjects  and  (ii) present that information in a manner that is clear and understandable.  Two sections of the JMB DP Policy Template require particular scrutiny to ensure that the descriptors match your school’s activities.  **Action One:**  Go to *Part 4: Processing Activities undertaken by the School* (page 4) and also refer to *Appendix 2: Personal Data and Related Processing Purposes* (pages 10 – 13.)  The template has identified the common processing activities a school engages in. For your school cross check those activities. If you carry out other data processing activities,  customise the template to reflect these additional activities and insert them in your policy document at Section 4, page 4 and in Appendix 2, (pages 10-13).  **Action Two**:  Go to *Appendix 3: Categories of Recipients* (on pages 14-15). If your school shares data with other recipients, please identify and describe who these are in your school’s policy and add these to Appendix 3,(pages14-15). |

|  |
| --- |
| **Communicating with Data Subjects** |
| Having customised the documentation, your school will then need to make this information available to the data subjects concerned.  This is likely to be best achieved through publication via your school website.  In line with best practice, the template policy aims to be as concise as possible. The primary intention is to avoid over-loading data subjects with too much information.  **Action One:**  Appendices 1-3 (pages 9-14) are considered integral to the Policy, and consequently should be readily available to data subjects.  **Action Two:**  Appendices 4-6 (pages 16-24) are primarily intended as operational guidance for school management and staff and schools may decide not to publish these beyond relevant staff |

## Part Two: Policy Review Activities

## Policy Review Process

In the tables following, we are suggesting a series of activities that can help to ensure that the policy review process is effective and brings meaningful benefits to the wider school community.

***Table One*** *relates to areas where some schools may already have initiated action.*

***Table Two*** *relates to customising your school’s transparency information*

|  |  |
| --- | --- |
| TABLE ONE | **Activities where some schools may already have initiated action.** |
| Raising Staff Awareness of GDPR | Promote awareness: schools need to be fully cognisant of their responsibilities with regard to GDPR principles such as accountability, transparency and confidentiality whenever personal data is being processed.  Data protection is, just like the area of Health & Safety, a whole-school responsibility that is shared amongst every member of the school community. An important first-step is to ensure that all staff are aware of their responsibilities. Confirm that each member of the school community is familiar with the content that is published on [www.GDPR4schools.ie](http://www.GDPR4schools.ie) This information has been tailored to different roles within the school (school board, senior management, teacher, admin support staff etc). |
| Undertaking a Data Processing Audit | Prepare a data processing inventory. This can be achieved by undertaking a *Data Audit* by answering questions such as:   * What personal data are we holding on students, parents, employees, past pupils? * When and how are we collecting this data? (applications, enrolment, educational assessments etc) * What other data is being created within the school? (school reports, incident reports etc)? * Where and how is the data stored? * Who within the school has access to the data? * How do we ensure the security of the data? * Do we take extra care with sensitive data (e.g. medical history, SEN data)? * What third parties are given access to school data?   Complete (or review) a Data Audit/Mapping Exercise: Ensure that your school has undertaken a Data Audit. Have the questions (above) been placed on an agenda for discussion and clarification?  Alternatively, has a questionnaire incorporating these questions been circulated for staff in key areas (e.g. Management, Year Heads, Special Needs, Guidance, School Office, IT, etc.) to consider.  The benefits of undertaking a data audit and/or data mapping exercise are significant.  For example, the process of undertaking an audit helps to raise general awareness amongst staff around important issues such as data storage and data security. Additionally, an audit will ensure the board of management has an understanding of all the data processing activities that are being undertaken under the board’s control. |
| Completion of a Risk Assessment Exercise | Your *Data Audit* provides the foundation for a *Risk Assessment* exercise, a GDPR requirement. Some guidance on the risk assessment process is provided under Integrity and Confidentiality in JMB DP Policy (Appendix 4 S.9 (pages 20-21)).Data controllers are expected to evaluate risk whenever they are processing personal data. As it is important that all staff have some understanding of the risks to which data subjects may be exposed, a Risk Assessment exercise is usually best undertaken on a whole-school basis.Complete a Risk Assessment: For each processing activity(a) list the associated risks(b) assess the level of each risk (how serious would its impact be?how likely is it to occur?)(c) prioritise the risk i.e. high/medium/low. |
| Risk Register and Mitigation | The outcome of any *Risk Assessment* exercise is a *Risk Register.* This may take the form of either a separate document or perhaps some additional column(s) added to a *Data Audit* table.  Under GDPR the controller must implement measures that ensure a level of security appropriate to any risk.  The completed *Risk Register* canthen form the basis for prioritising the follow-on action by the controller.  Examples of different types of measures that can be taken to mitigate risks include:   * technical e.g. regular software updates; security patches; antivirus software; strong firewall; secure storage of data backups; mobile device encryption; two-factor authentication for remote access etc. * physical e.g. locked offices; clean desk policies; functioning fire and burglar alarms; secure disposal of old laptops, computers and mobile devices. * organisational e.g. implementation of policies, training and procedures.  A risk assessment exercise is likely to emphasise security risks and potential data breaches. Any high probability, high impact risks will require immediate action to mitigate and control. Identify how best to address risks. Identify the measures and the resources needed to address risks. Prioritise the high risk areas for action. Refer to the guidance on Transparency provided in the JMB DP Policy Appendix 4 S.5 (page 16). |
| Data Sharing Arrangements | Another area of potential risk arises whenever personal data is legitimately accessed by non-school employees. While there are many situations in which such access is appropriate and necessary, it is the school’s responsibility to ensure that any data sharing with other recipients is carefully managed.  For example, where the data is being shared with another controller, the school will, need to confirm that an appropriate lawful basis has been identified to legitimise this sharing. Alternatively, when the data sharing arrangement is with a processor, such as a service provider, the school will need to confirm that the appropriate security guarantees have been given to the school and that a signed *Data Processing Agreement (DPA)* is in place*.*  Check *Data Processing Agreements*:  Identify any service providers who are processing personal data on behalf of the school. Confirm that there is an appropriate *Data Processing Agreement* in place, and that the service provider has provided a list of guarantees around security and other matters to the school (in line with GDPR Article 28 requirements). |
| TABLE TWO | Customising your school’s transparency information |
| Updating of Privacy Notices | Have data subjects been properly informed as to how their personal data is being collected, used and shared?  Confirm that Privacy Notices are in place: a template privacy notice has been published on [www.GDPR4schools.ie](http://www.GDPR4schools.ie) and this can be customised to reflect the school’s processing activities.  <https://gdpr4schools.ie/doc/exemplar_privacy_notice_to_students.docx> |
| Check your list of Processing Activities | While, a suggested list is set out in a concise manner in Section 4, page 4 of the template policy, GDPR transparency requirements mean that the level of detail provided in Appendix 2, (pages 10-13), should also be readily available (for example through an accessible link on the school website). Ultimately it will be for a school to decide what approach works best in each particular situation and context. There are likely to be some additional activities that are specific to each school (e.g. where the processing of personal data is being undertaken by the school for fundraising purposes etc). Identify all *Data Processing Activities*: Ensure that your Data Protection Policy is customised to your school. This means that you confirm that the list of purposes is an accurate reflection of your school processing activities. |
| Identify recipients | A list of common recipients of school data is provided in JMB Policy Appendix 3, (pages 14-16). Confirm Recipients: Ensure that your school’s list of recipients (or categories of recipients) is accurate. Confirm that an appropriate lawful basis has been identified to legitimise any sharing of personal data with other controllers. |
| Accountability | An emphasis on controller accountability is a central part of GDPR. This means a school should be able to demonstrate the steps it has taken to implement the legislation in general and the data protection principles in particular. This could include, for example, evidence of:   * an agreed Data Protection Policy * external training attended by school representatives * in-house training provided to school staff * inclusion of Data Protection on meeting agendas * outcomes of data audits and mapping exercises * risk assessment records * measures taken to address processing risks * copies of transparency information provided (privacy notices etc.) * evidence of consent forms * copies of Data Processing Agreements.  Collect Evidence: Create an “Accountability” file that collates and evidences the work done as the school progresses towards GDPR compliance. |

**Part Three: GDPR Autumn Training Schedule**

**Presenter: Cyril Drury, JMB Data Protection Advisor**

**Dates and Venues:**

|  |
| --- |
| Aug 15 Emmet House |
| Aug 21 Kilkenny Education Centre |
| Sept 30 Limerick Education Centre |
| Oct 9 Drumcondra Education Centre |
| Oct 18 Athlone Education Centre |
| Oct 22 Monaghan Education Centre |
| Nov 5 Blackrock Education Centre |

**Registration: Not yet open**