Data Protection by Design and Default Policy

St Aloysius Federated Primary School

Under the General Data Protection Regulation (GDPR), the school has a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Privacy by design should be a key consideration in the early stages of any project and should continue throughout its lifecycle. This allows schools to minimise privacy risks and builds trust. By designing projects, processes, products and systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage.
- Increased awareness of privacy and data protection across the school.
- The school are more likely to meet their legal obligations and less likely to breach GDPR.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

There are 7 foundational principles of privacy by design

- Proactive not reactive
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – Positive-sum, no zero-sum
- End-to-End security – Full lifecycle protection
- Visibility and transparency
- Respect for user privacy

1. Proactive not reactive

The Privacy by design approach is characterised by being proactive rather than reactive. By using this approach, the school will anticipate and prevent privacy invasive events before they happen. This approach means that the school are not waiting for a privacy risk to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short privacy by design comes before the fact, not after.

2. Privacy as the default setting

Privacy by design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy.

3. Privacy embedded into design.

Privacy by design is embedded into the design of school practices. It should not be a bolted add on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy becomes integral to school practices.

4. Full Functionality – Positive-Sum, not Zero-Sum

Privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade offs are made. Privacy by design avoids the pretence of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.

5. End-to-End security – Full lifecycle protection

Privacy by design, having been embedded into the project prior to anything else extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, privacy by design ensures cradle to grave, secure lifecycle management of information, end-to end.

6. Visibility and transparency

Privacy by design seeks to assure everyone that whatever the practice of the school regarding personal data that it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for user privacy

Above all, privacy by design requires the school the protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.