**GDPR data protection and processing checklist for governors**

The EU General Data Protection Regulations (GDPR), the new legal framework replacing the Data Protection Act 1998, will come into effect in the UK as of the 25 May 2018. Irrespective of the UK’s decision to leave the EU, the GDPR will still go forward. It is highly likely that the changes will result in schools needing to make amendments to their procedures regarding data protection and processing. This template has been created for governors, acting as a data protection and data processing checklist, to ensure that the correct procedures are in place at the school and are being implemented in compliance with the GDPR.

|  |  |  |
| --- | --- | --- |
| **Question for governors** | **Yes/no (if applicable)** | **Governors’ response** |
| Does the school have a written procedure for collecting personal data, which is compliant with the GDPR? |  |  |
| Does the school have a written procedure for using personal data, which is compliant with the GDPR? |  |  |
| Does the school have a written procedure for sharing personal data, which is compliant with the GDPR? |  |  |
| Does the school have a written procedure for storing personal data, which is compliant with the GDPR? |  |  |
| Does the school have a written procedure for disposing personal data, which is compliant with the GDPR? |  |  |
| How are the procedures for collecting, using, sharing, storing and disposing personal data shared with the relevant stakeholders, e.g. parents, pupils and staff? |  |  |
| How does the school evidence good data and information governance? |  |  |

|  |  |  |
| --- | --- | --- |
| **Question for governors** | **Yes/no (if applicable)** | **Governors’ response** |
| Do consent procedures meet the standards of the GDPR? |  |  |
| Has the school identified the data that requires consent? |  |  |
| Are the school’s procedures for obtaining consent for the usage of personal data (including explicit consent) compliant with GDPR? |  |  |
| With regards to obtaining consent, is consent a positive, unambiguous indication? Pre-ticked boxes and inferred from silence are non-compliant with the GDPR. |  |  |
| Is a consent record, documenting how and when consent was given, being utilised by the school? |  |  |
| Where a child is under the age of 16, **[or younger if the law provides it (up to the age of 13)]** have the parents given consent on behalf of their child, unless the processing is related to preventative or counselling services offered directly to a child? |  |  |
| Have areas at risk of data processing and protection breaches been identified and have these been managed/mitigated? |  |  |
| Does the school have a procedure for notifying the Information Commissioner Office (ICO) of significant data breaches within the specified timescale? **[This is currently set at 72 hours but is subject to change.]** |  |  |
| Has an assessment been undertaken to identify the types of data held, and which types of data would fall within the notification requirement, if there was a breach? |  |  |

|  |  |  |
| --- | --- | --- |
| **Question for governors** | **Yes/no (if applicable)** | **Governors’ response** |
| Does the school have a critical incident plan for if there is a data protection is breach? |  |  |
| Are there appropriate technical and organisational measures in place, so to demonstrate that data is processed in line with the principles set out in the GDPR? |  |  |
| Does the school have a comprehensive, clear and transparent **GDPR policy**? |  |  |
| Has the data protection officer (DPO) informed and advised the school and its employees about their obligations to comply with the GDPR and other data protection laws when handling and processing data? |  |  |
| Are sufficient resources supplied to the DPO to enable them to meet their data processing obligations? |  |  |
| Has the legal basis for processing data been identified and documented prior to data being processed, where relevant? |  |  |
| With regards to subject access requests (SARs), providing additional information, including data retention periods and the right to have inaccurate data corrected, does the school have an appropriate process that is complaint with the GDPR? |  |  |
| Are individuals aware that they have the right to submit a SAR, in order to verify their data is being processed lawfully? |  |  |
| Where SARs are made electronically, is the information provided in a commonly used electronic format? |  |  |

|  |  |  |
| --- | --- | --- |
| **Question for governors** | **Yes/no (if applicable)** | **Governors’ response** |
| Are all SARs fees based on the administrative cost of providing information, outlined in the GDPR? |  |  |
| Is there an identified process to inform an individual when personal information is disclosed to third parties? |  |  |
| Does the school have data processing agreements with all third parties that the school outsources data to? |  |  |
| If an individual requests for their data to be deleted and the personal data has been made public on an online format, has the school informed other organisations, who process the personal data, to erase links to and copies of the personal data in question? |  |  |
| Do the relevant school employees understand that an individual will be informed when a restriction on processing their data has been lifted? |  |  |
| How is the process for storing, sharing and disposing of data communicated with all staff, governors and volunteers? |  |  |
| Is the retention of data compliant with the GDPR? |  |  |
| Is the use of CCTV and photography complaint with the GDPR? |  |  |
| Do the correct employees have access to the School Information and Management System (SIMS)? |  |  |
| Do the correct employees have access to the school’s Single Central Record (SCR)? |  |  |

|  |  |  |
| --- | --- | --- |
| **Question for governors** | **Yes/no (if applicable)** | **Governors’ response** |
| Is there a record detailing who has access to what data? |  |  |
| Is this record reviewed on a regular basis to ensure it remains correct and compliant? |  |  |
| Is consistency in data processing and protection maintained across all departments and sites? |  |  |
| Does the school implement privacy by design in all its procedures, i.e. implementing privacy impact assessments? |  |  |

Checklist completed by: **Name**

Date: