GDPR and Data Protection Policy

February 2023

**POLICY STATEMENT**

We are committed to processing Personal Information fairly and lawfully in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (The DPA) and other related legislation which protects Personal Information. We recognise the importance of this and have updated our Policy to ensure that it gives effect to these important changes in the law.

As a School, it is necessary for us to process Personal Information about our staff, pupils, parent(s) / guardian(s) and other individuals who we may come into contact with. In doing so, we recognise that the correct and lawful treatment of Personal Information is critical to maintaining the confidence of those connected with our School.

This Policy has been written to reflect our ongoing commitment to promoting a strong culture of data protection compliance as well as safeguarding our children in accordance with the law.

**SAFEGUARDING STATEMENT**

Effective sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision to keep children safe. Serious case reviews (SCRs13) have highlighted that missed opportunities to record, understand the significance of and share information in a timely manner can have severe consequences for the safety and welfare of children.

We will be proactive in sharing information with relevant organisations as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children’s social care (e.g. they are being supported as a child in need or have a child protection plan). Staff should be alert to sharing important information in line with our Safeguarding Policy.

Information sharing is also essential for the identification of patterns of behaviour when a child is at risk of going missing or has gone missing, when multiple children appear associated to the same context or locations of risk, or in relation to children in the secure estate where there may be multiple local authorities involved in a child’s care. It will be for local safeguarding partners to consider how they will build positive relationships with other local areas to ensure that relevant information is shared in a timely and proportionate way.

**The Data Protection Act 2018 and General Data Protection Regulations (GDPR) do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.** To ensure effective safeguarding arrangements:

 • All organisations and agencies should have arrangements in place that set out clearly the processes and the principles for sharing information. The arrangement should cover how information will be shared within their own organisation/agency and with others who may be involved in a child’s life

• All practitioners should not assume that someone else will pass on information that they think may be critical to keeping a child safe. If a practitioner has concerns about a child’s welfare and considers that they may be a child in need or that the child has suffered or is likely to suffer significant harm, then they should share the information with local authority children’s social care and/or the police. All practitioners should be particularly alert to the importance of sharing information when a child moves from one local authority into another, due to the risk that knowledge pertinent to keeping a child safe could be lost

• The GDPR provides a number of bases for sharing personal information. It is not necessary to seek consent to share information for the purposes of safeguarding and promoting the welfare of a child provided that there is a lawful basis to process any personal information required. The legal bases that may be appropriate for sharing data in these circumstances could be ‘legal obligation’ or ‘public task’ which includes the performance of a task in the public interest or the exercise of official authority. Each of the lawful bases under GDPR has different requirements14. In some circumstances, it may be appropriate to obtain consent to share data but it is important to note that the GDPR sets a high standard for consent which is specific, 14 Further ICO guidance on lawful bases to share information can be found at Appendix B. 20 time limited and can be withdrawn (in which case the information would have to be deleted) 28. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, as provided for in the Data Protection Act 2018 and the GDPR.

To share information effectively:

• All practitioners should be confident of the lawful bases and processing conditions under the Data Protection Act 2018 and the GDPR which allow them to store and share information including information which is considered sensitive, such as health data, known under the data protection legislation as ‘special category personal data’

• Where practitioners need to share special category personal data, for example, where information obtained is sensitive and needs more protection, they should always consider and identify the lawful basis for doing so under Article 6 of the GDPR, and in addition be able to meet one of the specific conditions for processing under Article 9. In effect, the Data Protection Act 2018 contains ‘safeguarding of children and individuals at risk’ as a processing condition that allows practitioners to share information, including without consent (where in the circumstances consent cannot be given, it cannot be reasonably expected that a practitioner obtains consent or if to gain consent would place a child at risk). However, practitioners should be mindful that a data protection impact assessment for any type of processing which is likely to be high risk must be completed, and therefore aware of the risks of processing special category data

**GDPR Objectives**

* Monitoring compliance with data protection laws and our data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits.
* Advising on, and monitoring, data protection impact assessments.
* Cooperating and being the first point of contact with the Information Commissioner’s Office, members of staff, parents and pupils.

 **Lawful Processing**

Personal Information must be Processed lawfully. Under data protection laws, there are a number of grounds that make it lawful to Process Personal Information. We will only Process Personal Information if one or more of the following apply:

* The Data Subject has given his or her consent.
* The Processing is necessary for the performance of a contract with the Data Subject.
* The Processing is necessary to meet our legal obligations.
* The Processing is necessary to protect the Data Subject’s vital interests.
* The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (often referred to as Public Task).

 We recognise that some categories of Personal Information are more sensitive and further conditions must be satisfied if we are to Process this information (Special category and criminal conviction data). Where we Process these categories of Personal Information, we will ensure that we do so in accordance with the additional conditions for Processing set out under the GDPR and the DPA.

**Consent**

Where it is necessary for us to obtain consent to process Personal Information, we will ensure that we do so in accordance with data protection laws.

Generally, we will only obtain consent where there is not another lawful ground (see 6.1) for Processing. Some examples as to when we will obtain your consent is if we want to place a photograph of a pupil in the newspaper, on social media or in other publications to celebrate their achievements.

 We recognise that under data protection laws, there are stricter rules as to how consent is obtained. We will ensure that when we obtain consent, we: -

* Take steps to ensure that we make it clear to Data Subjects what they are being asked to consent to.
* Ensure that the Data Subject, either by a statement or positive action, gives their consent. We will never assume that consent has been given simply because a Data Subject has not responded to a request for consent.
* Never use pre-ticked boxes as a means of obtaining consent.
* Ensure that a Data Subject is informed that they can withdraw their consent at any time and the means of doing so.
* Keep appropriate records evidencing the consents we hold.

**Transparency**

We are required to provide information to Data Subjects which sets out how we use their Personal Information as well as other information required by law. We will provide this information by issuing Privacy Notices which will be concise, transparent, intelligible, easily accessible, and in clear, plain language.

**PROCESSING FOR LIMITED PURPOSES**

We will only collect and Process Personal Information for specified, explicit and legitimate reasons. We will not further Process Personal Information unless the reason for doing so is compatible with the purpose or purposes for which it was originally collected.

**ADEQUATE, RELEVANT AND LIMITED PROCESSING**

 We will only collect Personal Information to the extent that it is necessary for the specific purpose notified to the Data Subject.

 **ACCURATE DATA**

We will ensure that Personal Information we hold is accurate and kept up to date. We will also take all reasonable steps to ensure that personal information that is inaccurate is either erased or rectified without delay.

In supporting the School to maintain accurate records, staff, parents and other individuals whose personal information we may process are responsible for:

* Checking that any information that they provide to the School is accurate and up to date; and
* Informing the School of any changes to information that they have provided.

 **RETENTION**

We will not keep Personal Information for longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy and erase from our systems, all data which is no longer required. We will maintain a records retention schedule which will assist the School to destroy Personal Information once it is no longer necessary and in a safe and secure manner.

 **INDIVIDUAL RIGHTS**

We will process all personal Information in line with a Data Subject’s rights, in particular, their right to:

* Request access to any data held about them by the School.
* Rectification of inaccurate information.
* Erasure of Personal Information.
* Restrict the Processing of Personal Information.
* Object to the Processing of Personal Information.
* To receive Personal Information in a commonly used format (known as data portability) and have this transferred to another controller without hindrance.

 We will maintain a clear procedure detailing how such requests will be handled.

**DATA SECURITY**

We will implement appropriate technical and organisational measures to guard against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

 We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources and the level of risk identified.

 **PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS**

 We will integrate privacy by design measures when Processing Personal Information by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

 We will utilise Data Protection Impact Assessments (“DPIAs”) which will be used when introducing new technologies or the Processing is likely to result in a high risk to the rights and freedoms of Data Subjects.

 **ACCOUNTABILITY**

As a Data Controller, we are responsible for, and must be able to demonstrate, compliance with the data protection principles. Examples of how we will demonstrate compliance include (but are not limited to):

* Implementing policies and procedures e.g. a data protection policy, data breach procedures and subject access procedures.
* Undertaking information audits and maintaining a record of our processing activities in accordance with Article 30 of the GDPR.
* Preparing and communicating Privacy Notices to Data Subjects.
* Providing appropriate training at regular intervals.
* Implementing privacy by design when Processing Personal Information and completing data protection impact assessments where Processing presents a high risk to the rights and freedoms of Data Subjects.

**DISCLOSURE AND SHARING OF PERSONAL INFORMATION**

Where it is necessary to share Personal Information outside of the School, we will inform the data subject about this in accordance with this policy.

Examples of who we may share Personal Information with include other schools, the Local Authority and the Department of Education.