



Privacy Policy for Pembury Primary School

1. Introduction

1.1. This privacy policy sets out how Pembury Primary School uses and protects any information that you provide when using our school's services.

1.2. Pembury Primary School is committed to ensuring that your privacy is protected. All personal data collected will be used in accordance with this privacy statement and in compliance with data protection laws.

2. Information Collected

2.1. We may collect the following information:

- Names of students, parents, and staff
- Contact information including email addresses and phone numbers
- Demographic information such as postcode, preferences, and interests
- Other information relevant to student admissions, academic progress, and safeguarding.

3. How Information is Used

3.1. The information collected is used for the following purposes:

- Internal record keeping.
- Improvement of our educational services.
- Communication with parents/carers regarding student progress and school updates.

- Compliance with legal obligations.

4. Data Security

4.1. We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

5. Data Retention

5.1. We will only retain personal information for as long as necessary to fulfill the purposes we collected it for, including compliance with legal obligations.

6. Sharing Information

6.1. We do not sell, distribute, or lease personal information to third parties unless we have your permission or are required by law to do so.

7. Your Rights

7.1. You have the right to request access to the personal information we hold about you, to request correction of any inaccuracies, and to request erasure of your information.

8. Policy Review

8.1. This privacy policy is subject to regular review and may be updated without notice. Please check this page periodically to ensure you are aware of any changes.

New guidance (March 2024):

The Seven golden rules for sharing information (including personal information):

- 1. All children have a right to be protected from abuse and neglect. Protecting a child from such harm takes priority over protecting their privacy, or the privacy rights of the person(s) failing to protect them.** The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) provide a framework¹ to support information sharing where practitioners have reason to believe failure to share information may result in the child being at risk of harm.
- 2. When you have a safeguarding concern, wherever it is practicable and safe to do so, engage with the child² and/or their carer(s), and explain who you intend to share information with, what information you will be sharing and why.** You are not required to inform them, if you have reason to believe that doing so may put the child at increased risk of harm (e.g., because their carer(s) may harm the child, or react violently to anyone seeking to intervene, or because the child might withhold information or withdraw from services).
- 3. You do not need consent to share personal information about a child and/or members of their family if a child is at risk or there is a perceived risk of harm.** You need a lawful basis³ to share information under data protection law, but when you intend to share information as part of action to safeguard a child at possible risk of harm⁴, consent may not be an appropriate basis for sharing. It is good practice to ensure transparency about your decisions and seek to work cooperatively with a child and their carer(s) wherever possible. This means you should consider any objection the child or their carers may have to proposed information sharing, but you should consider overriding their objections if you believe sharing the information is necessary to protect the child from harm.
- 4. Seek advice promptly whenever you are uncertain or do not fully understand how the legal framework supports information sharing in a particular case.** Do not leave a child at risk of harm because you have concerns you might be criticised for sharing information. Instead, find out who in your organisation/agency can provide advice about what information to share and with whom. This may be your manager/supervisor, the designated safeguarding children professional, the data protection/information governance lead (e.g., Data Protection Officer⁵), Caldicott Guardian, or relevant policy or legal team. If you work for a small charity or voluntary organisation, follow the NSPCC's safeguarding guidance.
- 5. When sharing information, ensure you and the person or agency/organisation that receives the information take steps to protect the identities of any individuals (e.g., the child, a carer, a neighbour, or a colleague) who might suffer harm if their details became known to an abuser or one of their associates.**

6. **Only share relevant and accurate information with individuals or agencies/organisations that have a role in safeguarding the child and/or providing their family with support, and only share the information they need to support the provision of their services.** Sharing information with a third party rarely requires you to share an entire record or case-file – you must only share information that is necessary, proportionate for the intended purpose, relevant, adequate and accurate.
7. **Record the reasons for your information sharing decision, irrespective of whether or not you decide to share information.** When another practitioner or organisation requests information from you, and you decide not to share it, be prepared to explain why you chose not to do so. Be willing to reconsider your decision if the requestor shares new information that might cause you to regard information you hold in a new light. When recording any decision, clearly set out the rationale and be prepared to explain your reasons if you are asked.