



Wandsworth
Federation
of Maintained Nursery Schools

CPOMs Privacy Impact Statement

This policy was adopted by the Governing Body 23rd September 2026

This policy is due for review Autumn Term 2027

Signed:

(Chair of Governors)

Dated: 24th September 2024

Signed:

(Lead Head Teacher)

Dated: 24th September 2024

Privacy Impact Assessment (PIA) for:

CPOMS Systems Limited

Data Protection Principles

- Ⓢ processing to be lawful and fair
- Ⓢ purposes of processing be specified, explicit and legitimate
- Ⓢ adequate, relevant and not excessive
- Ⓢ accurate and kept up to date
- Ⓢ kept for no longer than is necessary
- Ⓢ processed in a secure manner

Why we need a Privacy Impact Assessment – screening questions?

We need to complete this form because:

- Ⓢ the use involves the collection of new information about individuals;
- Ⓢ the use compels individuals to provide information about themselves;
- Ⓢ the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information;
- Ⓢ we are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Ⓢ we are using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition;
- Ⓢ the use results in you making decisions or acting against individuals in ways that can have a significant impact on them;
- Ⓢ the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private;
- Ⓢ the use requires you to contact individuals in ways that they may find intrusive.

Describe the service

CPOMS is a software system which enables the recording and sharing of Safeguarding Information, including attendance and behavioural information re children and families at our School. We need to complete the PIA because of the sensitivity of the data held.

Describe the data collected and the possible uses of the data

Lists of data held The data held is that put onto the system by staff and is therefore difficult to define (see possible uses). It may include names, dates of birth, family names and contact information, safeguarding, behavioural and attendance concerns. Minutes from meetings.	Collection of data The data will be placed onto the systems by individual staff either by completion of online forms or by the uploading of linked documentation Possible uses Documents about individuals or families contain personal data. To support completion of Safeguarding Forms and referrals. To share concerns with other establishments who use CPOMS and have siblings at their school.
---	--

Identify the privacy, related risks and possible solutions

Privacy issue	Risk to individuals	DPA Risks	Possible Solutions
⊗ Personal data shared with the wrong person ⊗ Information added to wrong child's account ⊗ Data not held securely ⊗ Data viewed by person who not	⊗ Disclosure to person who is not authorised to see it ⊗ Wrong information linked to the individual ⊗ Wrong person being	⊗ Unauthorised access to data ⊗ No knowledge of data breach and therefore lack of reporting ⊗ Data Breach because	⊗ Access carefully controlled through passwords and application of restricted access. ⊗ Reminders in staff meetings ⊗ Encourage reporting of breaches ⊗ Staff should be informed of correct practices

see it	able to access data ⊗ Wrong person given access to data	wrong information linked to individual, and possibly shared. ⊗ Data breach caused by unauthorised access to data ⊗ Data breach caused by unauthorised access to data	in completing 'concerns': ▪ Checking name of child ▪ Check correct documents uploaded. ⊗ Confirm with hosting company security and storage of data, not held outside of EU. ⊗ Staff to be given clear instructions to lock computer screens ⊗ Not to use computers which could be in view of visitors
Sign off and notes			
Comments on risks		Processes that must be in place	
Risk around ensuring correct data is linked to the correct person		Staff to be given clear training re CPOMS. Members of DSL Group receive e mail notification of every concern added so double checks will be made.	
Many of the risks can be handled by a session during the induction process of the user		Training during Induction to be detailed, re use of CPOMS and Data Protection	
Data accessed by wrong person		All staff have personal log ins both to the network and to CPOMS, and access is restricted by role. Higher access to Designated Leads	

Contact point for future privacy concerns

Data Protection Officer:

Data Protection Lead:

Date completed:

13/02/2019