

CPOMS Systems Limited

Information to assist in Supplier Due Diligence and DPIAs

We receive large numbers of requests from schools and other customers, asking us to complete a compliance and/security questionnaire as part of their due diligence process or seeking information to help with a Data Protection Impact Assessment.

We are unable to complete them individually but, as they all request the same information, we are making that information available here in this webpage.

User notes

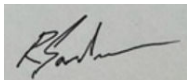
The following information applies to all CPOMS services, unless otherwise stated, so references to “CPOMS”, “CPOMS systems” and “CPOMS data” should be read accordingly.

Please note, this is not a Data Protection Impact Assessment (DPIA). The information is intended only to help you, as a Controller, to perform due diligence, monitor supplier (our) compliance, and complete a DPIA on your safeguarding processes, for which you use CPOMS.

Nothing in this document changes any provisions of the [CPOMS Terms & Conditions](#) under which we provide our CPOMS services to you.

The information is accurate to the best of our knowledge and belief and is provided in good faith. However, CPOMS Systems Limited accepts no liability for any errors or omissions or for any consequences of decisions made in reliance on it.

I trust that you will find this information useful but, if there is anything further you require, please do not hesitate to contact our Data Protection Officer at dpo@cpoms.co.uk.



Richard Gardner

Managing Director

CPOMS Systems Limited.

20th November 2024

Contact Email: support@cpoms.co.uk

Information about CPOMS to help you complete Due Diligence and DPIAs

CPOMS Terms & Conditions

What Terms and Conditions apply to us? Follow this link to the [CPOMS Terms & Conditions](#) landing page and bookmark it for future reference.

From the landing page, click the applicable button or buttons. These will take you to the relevant terms for each service (e.g. StudentSafe, StaffSafe), either you are an educational, a non-educational setting or a Local Authority, and whether you are an individual setting or a group of settings, such as a Multi-Academy Trust.

What about changes to the Terms & Conditions? Clause 19 Variations permits us to make changes and where the change has a material impact on you, we much give you written notice.

While you can download PDF copies of our T&Cs, you should always check online for the current version.

Will we also need a 'data processing agreement' (DPA)?

No. The CPOMS T&Cs constitute a data processing agreement.

A leading law firm drafted the terms and conditions specifically to ensure that they meet all the UK GDPR requirements for a data processing agreement, including the Controller's 'written instructions' to its Processor, and all the clauses mandated by Article 28.

Will we also need a 'data sharing agreement' (DSA)?

No. A "data sharing agreement" is required when a Controller shares personal data with another Controller for the latter to use for its own purposes.

You are not "sharing" data with us – you are instructing us to "process" it for you, (see [ICO Guidance](#)) so ours is a Controller to Processor relationship.

Governance

What Governance do you have in place to protect our data?

We have implemented a comprehensive Privacy Programme, which is overseen by our Information Governance Committee and our Data Protection Officer.

The IGC keeps the Risk Register under constant review and ensures that Risk Owners regularly monitor their risks and review the controls they have implemented to mitigate them.

Records of Processing Activities

Do you have a Record of Processing Activities? We use Privacy Management Software, which holds our two Records of Processing Activities – one documenting our activities as a Controller and the other documenting our activities as a Processor.

Privacy & Security Training

Do your relevant employees receive regular Privacy and Security training? Yes. Security and Privacy training is provided at induction with regular refreshers at least annually.

Implementation of CPOMS

How is CPOMS implemented? The implementation procedure is described in the Services schedule of the [CPOMS Terms & Conditions](#) See also “Data Collection” below.

Will our staff need training? Yes. Training resources are available on request. All training is online.

Will CPOMS require any manual input? If yes, what will this be? If your MIS or equivalent system is not compatible with CPOMS or any of the integrators (e.g. Groupcall, Wonde), the data import may need to be done manually. This does not require significant effort on your part.

How long is the implementation process? When we have received your basic setup information and your first MIS link, your system will be built and ready to use within two working weeks.

Data to be Processed

What categories of data will you process? You decide what categories of personal data to import into CPOMS, e.g. from your MIS, and your authorised users decide what information to enter and what files to upload when logging a concern or incident.

Schedule 1 of the [CPOMS Terms & Conditions](#) sets out processing details.

How will you collect and store the data? Data is migrated into CPOMS via secure (encrypted) data import from your Management Information System (MIS) or equivalent system, either directly, using your MIS/system’s API or by engaging an integrator.

Additional information will be entered by your authorised users, e.g. when reporting a safeguarding incident.

All data is encrypted and stored in the UK in Microsoft Azure datacentres.

Subcontractors / Sub-processors

Do you use subcontractors for any part of the service?	<p>Yes. The CPOMS Terms & Conditions include provisions that govern our use of sub-processors.</p> <p>Our subcontractors are listed in Schedule 2 of the CPOMS Terms & Conditions. The CPOMS systems are hosted and backed up in Microsoft Azure, in two UK datacentres.</p> <p>Where CPOMS is unable to integrate directly with a school's MIS, we ask you to engage an integrator – usually Groupcall (Community Brands) or Wonde but other providers are available if you prefer.</p>
If so, do their contracts comply with UK GDPR, including Art. 28?	<p>Yes, we have reviewed our contracts with Microsoft, Wonde and Community Brands and confirm they meet the requirements of the UK GDPR and contain the clauses mandated by Art. 28.</p>
How do you monitor compliance with their contractual and legal obligations?	<p>We perform an annual review of the relevant documents on the Microsoft Service Trust Portal and we require Wonde and Community Brands to complete Supplier Privacy & Security Audit Self-Assessment in accordance with our Controls Review Schedule.</p>
What elements of our data can your sub-contractors access?	<p>Microsoft, which provides the hosting service, has access to encrypted data as necessary to provide their hosting service, but they cannot decrypt the data because CPOMS Systems Limited manages its own encryption keys.</p> <p>If you need help to migrate data from your MIS into CPOMS, we will engage an integrator. The integrator will need access to the data on your MIS so they can migrate the categories of data you have selected to CPOMS, but they will have no access to any data in CPOMS.</p>
In the event of a breach can you compel your sub-contractors to assist you?	<p>Yes, they have the same contractual obligations to us as we have to you, and they are also subject to the UK GDPR.</p>

Data Subject Requests (e.g. Subject Access Requests, aka SARs, DSARs)

What do you do if you receive a Data Subject Request from a student, parent or member of staff?	<p>We refer them to the applicable school/organisation, explaining that we are unable to access the information for them.</p>
---	---

Would you provide us any support we might need to complete a Data Subject Request that we receive?

Yes, we would talk you through how to access and provide the data that is being requested but we have very restricted access to your data so are unable to do more than that.

Can you compel your sub-contractors to assist with a data subject request?

Contractually yes. However, in practice, they would be unable to assist because Microsoft cannot access unencrypted data and Community Brands or Wonde have no access to any data in the CPOMS systems.

Personal Data Breaches

If there is a breach of your system that involves our data, when and how will you notify us?

We are contractually obliged to notify you of a breach “without undue delay (and within 24 hours wherever possible)”

Notification would be by email, phone call or via the CPOMS system, depending on the number of affected schools or customers.

If requested, would you provide information to help with a breach investigation?

Yes.

Security

Do you hold ISO 27001 or other recognised security certification

Yes. ISO/IEC 27001:2002 Certificate ID No. 10570075 issued by UKAS-accredited auditors Lloyds Register Quality Assurance (LRQA).

Microsoft Azure, which hosts CPOMS is also [ISO-27001 certified](#).

What security measures do you have in place to protect our data?

Having appropriate, adequate and proportionate measures in place is both CPOMS’s legal obligation as a processor under Article 32 of the UK GDPR, and our contractual obligation to you under Clause 10.4.4 of the [CPOMS Terms & Conditions](#).

Details of security measures may be found in Schedule 3, s.3 Information Security in the [CPOMS Terms & Conditions](#).

For security reasons, CPOMS Systems Limited does not publish full details of its security arrangements; however, we can confirm that we have appropriate and proportionate security measures in place that meet our legal and contractual obligations to you, and that we monitor security threats and our security measures on a continuous basis.

How do you control access to our data?

We apply strict role-based access permissions. A limited number of engineers (usually no more than four) have privileged access to the systems which enables access to your data. Such access is incidental only

and limited to what is necessary to complete their tasks, which include maintaining the service and supporting your authorised users.

Anonymised and less sensitive records (user accounts, email addresses, system configuration), can be accessed and modified by CPOMS employees to varying degrees via role-based access permissions and other controls, including access and activity logging.

Access by your authorised users may be controlled (at your discretion) by multi-factor authentication (MFA), requiring them to enter their user ID, a strong password and a code from an authenticator app or USB key.

How do you test security of the CPOMS systems?

Our external security testing approach is built around the concept of 'continuous assurance', combining regular penetration test with a "bug bounty" programme. The aim of this dual approach is to ensure that our systems are constantly being tested for security vulnerabilities, while also ensuring a high degree of rigour.

We have rigorous automated testing of all code at every pre-production stage. This includes static code analysis and patch-level security scanning of dependencies. In addition, our infrastructure undergoes continual automated scanning, externally and internally focused.

Business Continuity & Disaster Recovery

What measures are in place to recover from a disaster or other unplanned outage at the CPOMS datacentre?

The CPOMS systems and databases are hosted on servers across two geographically separate Microsoft Azure data centres to maximise resilience and availability. Both data centres are in the UK.

The live systems and databases are mirrored in the second datacentre, providing a complete failover in the event of an unplanned outage at the first datacentre.

As required under our ISO27001 certification, the policies and procedures covering both preparation for and response to security incidents, breaches, disasters and other unplanned outages impacting the confidentiality, integrity and availability of the CPOMS systems and the databases containing your data, are all documented with our Information Security Management System, as well as our Business Continuity, Incident Response and Disaster Recovery Plans and our Breach Notification Procedures.