PSP ASSET PROTECTION

Privacy Policy

Clear information about how we use and protect personal data

Policy owner	Managing Director / Data Protection Lead
Effective date	1st November 2026
Review date	November 2027 or earlier if our processing or the law changes
Applies to	Website visitors, business contacts, customers, suppliers and people whose data we process for customers

At a glance

- We use business contact data to answer enquiries, supply and support our products, manage accounts and meet legal obligations.
- For direct business-to-business marketing, we normally rely on legitimate interests and always provide a simple way to opt out.
- When we support a school's Infiniti library management system, the school controls pupil and staff data; PSP processes it only for the school and never uses it for marketing.
- We do not sell personal data.
- You can contact us to exercise your rights or complain about how we have used your personal data.

This policy is intended to meet the transparency requirements of UK data protection law. It should be read with any service-specific terms, data processing agreement and our Cookie Policy.

1. Who we are

PSP Asset Protection Limited ("PSP", "we", "us" or "our") is responsible as controller for the personal data described in this policy, except where we act as a processor for a customer as explained in section 9.

Detail	Information
Legal name	PSP Asset Protection Limited
Company number	07852228
Registered office	47 Butt Road, Colchester, Essex, CO3 3BZ, United Kingdom
Trading address	Unit 2 Manor Farm Business Centre, Manor Lane, Stutton, Ipswich, IP9 2TD, United Kingdom
Privacy contact	Managing Director / Data Protection Lead
Email	info@psp-assetprotection.co.uk
Telephone	01473 745375
ICO registration	ZA340807

We are not required to appoint a statutory data protection officer. Our Data Protection Lead coordinates privacy matters and can be contacted using the details above.

2. Scope

This policy applies when you visit our website, enquire about or buy our products and services, receive support, work with us as a supplier or partner, apply for a role, or otherwise communicate with PSP. It also explains our limited role when we process personal data for a school, academy, college, library or other customer.

A customer's own privacy notice applies to the personal data it controls, including pupil, student, borrower and staff records held in a library management system. Our Cookie Policy provides more detail about cookies and similar technologies used on our website.

3. Data we collect

Category	Examples
Identity and contact data	Name, job title, organisation, work email, telephone number and postal address. We only collect business rather than home contact details.
Commercial and account data	Enquiries, quotations, orders, contracts, licenses, warranties, delivery details, invoices, payment status and account correspondence. We do not store full payment-card details.
Support and technical data	Support tickets, fault details, device identifiers, system configuration, diagnostic information, remote-support session metadata and communications with our support team.
Website and device data	IP address, browser and device type, referring pages, pages viewed, cookie identifiers and basic interaction data, subject to your cookie choices.
Marketing and preference data	Areas of business interest, event or demonstration attendance, communication preferences, opt-outs and responses to campaigns or surveys.
Supplier and partner data	Business contact, due-diligence, contract, delivery and payment information for our suppliers, manufacturers, resellers and service partners.
Recruitment data	CV, work history, qualifications, contact details, interview notes, references and right-to-work information where relevant.

Category	Examples
Rights and complaint data	Identity evidence where necessary, details of a request or complaint, correspondence, investigation records and outcomes.

We do not intentionally collect special category data (such as health information, ethnicity, religious or political beliefs, trade-union membership, sexual orientation, genetic or biometric data) for our own business purposes. Please do not send it unless we have specifically asked for it and explained why it is needed. If such data appears in customer-controlled records that we support, we process it only on the customer's documented instructions and subject to the applicable data processing agreement.

4. How we obtain data

We collect personal data:

- directly from you, for example through email, telephone calls, forms, meetings, demonstrations, orders, support requests, events or remote-support sessions;
- from your employer, school, trust, college, library, purchasing organisation, reseller or other business contact;
- from publicly available professional sources, organisation websites, procurement portals and business directories;
- from our authorised partners, suppliers and service providers where this is necessary to deliver a service; and
- automatically from our website and systems, subject to cookie and device settings.

If we obtain your data from another source, we will provide appropriate privacy information within the period required by law, unless an exemption applies or you already have that information.

5. Uses and lawful bases

We use personal data only where we have a lawful basis. More than one basis may apply, depending on the context.

Purpose	Lawful basis
Respond to enquiries, prepare quotations and take steps requested before a contract	Contract or steps before contract; legitimate interests in developing our business and responding to organisations.
Process orders, install products, provide licences, maintenance, training and support, and manage the customer relationship	Contract; legitimate interests where the contract is with your organisation rather than you personally.
Administer invoices, payments, tax, insurance, audits and company records	Legal obligation; contract; legitimate interests in sound financial administration and protecting our legal position.
Operate and secure our website, CRM, email, support and business systems; diagnose faults and prevent misuse	Legitimate interests in operating secure, reliable services; recognised legitimate interests or legal obligation where applicable to security or crime prevention.
Provide remote support, including authorised unattended access where agreed	Contract; legitimate interests in resolving faults efficiently and maintaining supported equipment.
Send relevant B2B information about products, services, webinars, events and customer updates	Legitimate interests in marketing our services to relevant professional contacts; consent where required by the Privacy and Electronic Communications Regulations.
Analyse service use, customer feedback and campaign performance to improve our products and support	Legitimate interests in service improvement and business planning; consent for non-essential cookies or similar technologies where required.
Manage suppliers, partners, resellers and professional advisers	Contract; legitimate interests in managing our supply chain and commercial relationships.
Recruit staff or contractors	Steps before contract; legitimate interests in recruitment; legal obligation for required checks.

Purpose	Lawful basis
Handle rights requests, complaints, disputes, claims and regulatory enquiries	Legal obligation; legitimate interests in resolving concerns and establishing, exercising or defending legal claims.
Comply with court orders, law-enforcement requests and other legal requirements	Legal obligation; recognised legitimate interests where the law permits and the processing is necessary.

Where we rely on legitimate interests, we consider the purpose, necessity and impact on individuals. You may object to processing based on legitimate interests; see section 13. Where we rely on consent, you may withdraw it at any time without affecting processing already carried out.

6. B2B marketing

We may use professional contact details to send relevant information to customers and other organisations that may reasonably be interested in library technology, asset protection, RFID, self-service, library management systems, support and related services. We do not sell or rent marketing lists.

You can opt out at any time by using the unsubscribe link in an email or contacting info@psp-assetprotection.co.uk. We may keep a minimal suppression record so that we can respect your choice. Service messages about an existing contract, security issue, system availability or essential product update are not marketing and may still be sent where necessary.

7. Sharing personal data

We share personal data only where necessary, proportionate and subject to appropriate safeguards. Recipients may include:

- technology and hosting providers supporting our website, email, CRM, cloud storage, support desk, remote-support and security services;
- product manufacturers, software licensors and service partners, including Concord Australia Pty Ltd where this is necessary to supply or support Infiniti;
- delivery, installation, training and engineering partners;
- accountants, insurers, banks, auditors, legal advisers and other professional advisers;
- public authorities, regulators, courts, law-enforcement bodies or fraud-prevention organisations where disclosure is required or permitted by law;
- a prospective buyer, investor or successor if our business or assets are reorganised, sold or transferred, subject to confidentiality and due diligence controls; and
- other parties where you have asked us to share the data or have given valid consent.

Where a supplier processes personal data for us, we require an appropriate written contract and proportionate security and confidentiality measures. We do not allow processors to use the data for their own unrelated purposes.

8. Remote support

We may use approved tools such as Zoho Assist, TeamViewer or Windows Quick Assist to diagnose and resolve technical issues. Remote support is started with an authorised user's knowledge, except where the customer has agreed in writing to controlled unattended access for supported equipment such as self-service kiosks.

- Access is limited to trained and authorised personnel and to what is reasonably necessary for the support task.
- Customers should close unrelated records and applications where practical before a session and should not provide unnecessary pupil, borrower or special category data.
- Session metadata may include the date and time, customer or device identifier, support agent, duration and connection details. The exact information depends on the approved tool and configuration.
- We do not routinely record screen contents or copy files. If recording or file transfer is needed, we will explain this and obtain the appropriate authority before proceeding.
- Unattended access is subject to documented customer authorisation, access controls and periodic review, and may be withdrawn in accordance with the support agreement.

9. School and customer data

When we supply and support systems such as the Infiniti library management system, the school, academy trust, college, library or other customer normally decides why and how pupil, student, borrower and staff data is used. The customer is the controller and PSP acts as its processor.

- We process that data only on the customer's documented instructions and under a written data processing agreement.
- We use the data only to implement, migrate, host where applicable, maintain and support the service. We never use pupil, student, borrower or staff records for PSP marketing.
- We use approved sub-processors where needed to provide the service and flow down appropriate data-protection obligations. Details are provided in the relevant data processing agreement or sub-processor information.
- Temporary working copies used for import or migration are securely deleted within seven days after successful import, unless the customer instructs otherwise or a documented exception is required to resolve an issue.
- We assist customers, as reasonably required, with rights requests, security incidents, data protection impact assessments and other compliance duties.
- Questions or rights requests about records held by a school or other customer should normally be sent to that organisation first. We will help the customer respond.

The customer's own privacy notice explains its purposes, lawful bases, retention periods and how individuals can exercise their rights in relation to those records.

10. International transfers

Some suppliers or their support teams may be located outside the United Kingdom, or may allow access to personal data from outside the United Kingdom. In particular, Concord Australia Pty Ltd is based in Australia and may be involved in the provision and support of Infiniti. Australia is not currently covered by UK adequacy regulations.

We do not make or permit a restricted transfer unless it is covered by a lawful transfer mechanism. Depending on the destination and circumstances, this may include:

- UK adequacy regulations, including an applicable approved framework or sector;
- the UK International Data Transfer Agreement (IDTA);
- the UK Addendum to the EU Standard Contractual Clauses; or
- another safeguard or limited exception permitted by UK data protection law.

Where an appropriate safeguard is required, we also complete or obtain an appropriate transfer risk assessment and apply supplementary technical or organisational measures where needed. You may contact us for further information about relevant destinations and safeguards; commercially sensitive information may be redacted.

11. Retention

We keep personal data only for as long as reasonably necessary for the purpose collected, including to meet contractual, legal, tax, accounting, insurance, security and dispute-resolution requirements. Our standard periods are below; a shorter or longer period may apply where the context, contract, customer instruction, legal obligation or documented risk requires it.

Record	Standard retention
Enquiries, demonstrations and unsuccessful quotations	Up to 24 months after the last meaningful contact, unless a longer period is justified by an active procurement or you ask to remain in contact.
Customer contracts, orders, account records and material service correspondence	For the relationship and normally six years after it ends.
Invoices, payment and tax records	Normally six years after the end of the relevant financial year, or longer where required by law.
Support tickets and service history	For the support relationship and normally six years after closure where needed to evidence service delivery; routine diagnostic attachments may be deleted sooner.

Record	Standard retention
Remote-support session logs	Normally 24 months, unless a contract, security investigation or legal claim requires longer.
Marketing contacts and preferences	Until you opt out or after 24 months without meaningful engagement; a minimal suppression record may be kept to respect an opt-out.
Website analytics and cookie data	For the period stated in our Cookie Policy or consent tool and normally no more than 14 months for identifiable analytics data.
Rights requests and data-protection complaints	Normally six years after closure to demonstrate how the matter was handled.
Unsuccessful recruitment records	Normally six months after the decision, unless a longer period is agreed or needed for a legal claim.
Temporary customer import or migration files	Within seven days after successful import, subject to a documented exception or customer instruction.
Customer-controlled LMS data	As instructed by the customer and set out in the service contract or data processing agreement; return or deletion follows the agreed end-of-service process.

When retention ends, we securely delete or anonymise the data. Backup copies are removed through the normal backup lifecycle. We may suspend deletion where records are needed for a complaint, investigation, litigation hold or other legal requirement.

12. Security

We use proportionate technical and organisational measures designed to protect personal data against accidental or unlawful loss, alteration, disclosure, access or destruction. Measures include, where appropriate:

- role-based access and least-privilege controls;
- multi-factor authentication for relevant cloud and administrative systems;
- encryption in transit and, where supported and appropriate, at rest;
- managed anti-malware, security updates, firewalls and device controls;
- encrypted company devices and secure disposal;
- approved business systems, including Zoho services, our email provider and approved cloud storage;
- supplier due diligence, contracts and access restrictions;
- staff confidentiality, awareness and incident-reporting procedures; and
- backup, continuity and recovery arrangements appropriate to the service.

No method of transmission or storage is completely secure. If we identify a personal data breach, we follow our incident procedure, contain and assess it, notify an affected controller without undue delay where we act as processor, and make any legally required notifications to the ICO and affected individuals.

13. Your rights

Depending on the circumstances, UK data protection law gives you the right to:

- **Be informed** about how your personal data is used;
- **Access** your personal data and receive a copy;
- **Rectify** inaccurate or incomplete personal data;
- **Erase** personal data where the legal conditions apply;
- **Restrict** processing in certain circumstances;
- **Data portability** for data you provided where processing is automated and based on consent or contract;
- **Object** to processing based on legitimate interests and at any time to direct marketing;
- **Withdraw consent** where consent is the lawful basis, without affecting earlier lawful processing; and
- **Challenge qualifying automated decisions** and request human intervention where the law gives that right.

PSP does not make decisions about you that have legal or similarly significant effects solely by automated means as part of the processing described in this policy.

To exercise a right, email info@psp-assetprotection.co.uk or write to our trading address. Rights requests are normally free. We may ask for information needed to confirm your identity or clarify the request. We will respond without undue delay and normally within one month; the period may be paused or extended where the law permits. We may charge a reasonable fee or refuse a request only where legally allowed, for example if it is manifestly unfounded or excessive.

If PSP holds the data only as a processor for a school or other customer, we will normally pass the request to that controller and assist it in responding.

14. Data complaints

You have the right to complain to PSP if you believe we have not handled your personal data in accordance with data protection law. Please send the details, relevant dates and any supporting information to info@psp-assetprotection.co.uk, with "Data protection complaint" in the subject line, or write to our trading address.

We will acknowledge a data protection complaint within 30 days, investigate it without undue delay, keep you appropriately informed and explain the outcome. We may ask for information needed to understand the issue or confirm identity or authority.

You may also complain to the Information Commissioner's Office (ICO), although the ICO normally recommends giving us an opportunity to address the concern first:

ICO contact	Details
Website	https://ico.org.uk/make-a-complaint/
Telephone	0303 123 1113
Address	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

15. Cookies

Our website uses cookies and similar technologies. Strictly necessary technologies may operate without consent where the law allows. We ask for a clear choice before setting non-essential analytics, functionality or advertising technologies where consent is required. You can change or withdraw your choices through the website's cookie controls and browser settings.

Our Cookie Policy explains the cookies in use, their providers, purposes and durations. We do not rely on continued browsing as consent to non-essential cookies.

16. Children

Our website and direct sales activities are aimed at organisations and professional users, not children. We do not knowingly collect children's personal data directly for marketing. Where children's data is present in a system supplied to a school or college, the customer is responsible for the purpose and lawful basis and PSP acts only as a processor as described in section 9.

17. Changes

We review this policy at least annually and when our services, suppliers, processing or legal obligations change. The current version will be published on our website with its effective date. If a change materially affects how we use personal data, we will take reasonable steps to bring it to the attention of affected people.

18. Contact us

For privacy questions, rights requests or data protection complaints, contact:

Managing Director / Data Protection Lead

PSP Asset Protection Limited
Unit 2 Manor Farm Business Centre
Manor Lane, Stutton
Ipswich, IP9 2TD
Email: info@psp-assetprotection.co.uk
Telephone: 01473 745375

Document control: Version 2.0 • Effective 28 October 2026 • Next scheduled review October 2027 • Approved by the Managing Director.