Data Privacy Notice – Clients and Service Delivery

Document name Data Privacy Notice – Clients and Service Delivery	Reference	
Created by Glyn Pascoe	**Issue date** June 2026	
Review date Annually	**Review date** June 2027	
Protection status Public	**Issue no.** 2.4	**Page no.** 1 of 7

Introduction

Under data protection law, individuals have the right to be informed about how iCT4 Limited uses any personal data we hold or come into contact with. We comply with this right by providing this Privacy Notice.

This notice covers two distinct roles that iCT4 Limited carries out in relation to personal data:

- Data Controller – where iCT4 decides the purposes and means of processing. This applies to personal data about named individuals at client and prospective client organisations (for example, headteachers, IT coordinators, business managers) held for commercial purposes such as account management, billing, and marketing.
- Data Processor – where iCT4 may access or come into contact with personal data owned and controlled by a client organisation in the course of providing technical support or other contracted services. In this role iCT4 acts on the client's instructions. The client organisation remains the data controller and retains full responsibility for that data.

This notice is issued in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025 (DUAA 2025).

Who we are

iCT4 Limited, with registered address at Trevenson House, Church Road, Pool, Redruth, Cornwall, TR15 3PT, is the Data Controller for client contact data as described in this notice. Our Data Protection Representative (DPR) is responsible for ensuring this notice is made available to data subjects prior to iCT4 collecting or processing their personal

www.ict4.co.uk hello@ict4.co.uk
01209 311344 Trevenson House, Church Road, Redruth, TR15 3PT

data. All employees of iCT4 Limited who interact with data subjects are expected to direct them to this notice.

Part A: iCT4 as Data Controller — client contact data

This part covers personal data that iCT4 holds about individuals at client and prospective client organisations for the purposes of the commercial relationship.

Personal data we hold about you

This may include, but is not restricted to:

- Contact details: full name, title, job role, email address, telephone numbers, and business address
- Financial details: bank account information for processing payments and invoicing
- Technical details: usernames and credentials used in service account management
- Recordings: screen recordings made during remote support sessions
- Marketing data: communication preferences, event attendance, and consent records
- CCTV footage recorded at iCT4 offices
- Data about your use of iCT4's information and communications systems

We do not routinely collect special category data (such as health, ethnicity, religion, or biometric data) about client contacts. Where this arises we will only process it where the law allows.

Why we use this data and our lawful basis

We use client contact data for the following purposes, relying on the lawful bases shown:

- Fulfilling and administering service contracts — lawful basis: contract
- Communicating about your account, services, and support requests — lawful basis: contract
- Processing payments and managing billing — lawful basis: contract and legal obligation
- Meeting our legal and regulatory obligations — lawful basis: legal obligation
- Fraud prevention and network security — lawful basis: legitimate interests (Article 6(1)(f) UK GDPR)
- Direct marketing to existing clients — lawful basis: legitimate interests and the PECR soft opt-in. You may opt out at any time.
- Direct marketing to new contacts — lawful basis: consent. You may withdraw consent at any time.
- Safeguarding or emergency response — lawful basis: recognised legitimate interests under the DUAA 2025, where no balancing test is required

Direct marketing and PECR

Where we contact you by email for marketing purposes, we do so in compliance with the Privacy and Electronic Communications Regulations (PECR). For existing clients we rely on the soft opt-in, meaning we may contact you about relevant services provided you

www.ict4.co.uk hello@ict4.co.uk
01209 311344 Trevenson House, Church Road, Redruth, TR15 3PT

have a clear opportunity to opt out at any time. For new contacts we require consent first. You can unsubscribe from any marketing communication by contacting our DPR or using the unsubscribe link in any email we send.

How we collect this data

We collect contact data via phone, post, email, and in person. Common collection points include:

- Helpdesk account sign-up
- Service or product applications
- Newsletter or event subscriptions
- Trade shows and promotional events

Part B: iCT4 as Data Processor — service delivery

When iCT4 provides technical support and managed IT services, our engineers may, in the course of that work, access or have sight of personal data held on client systems. Under UK GDPR, any access to personal data constitutes processing, even where that access is incidental to the technical task being carried out. In this capacity iCT4 acts as a data processor. The client organisation is, and remains, the data controller for that data and is responsible for its lawful basis and for fulfilling data subject rights.
The nature of our access varies by service. Two common scenarios are:

- Technical support and troubleshooting — engineers may remotely access a client's systems or network to diagnose and resolve issues. During this access they may incidentally have sight of personal data held in those systems. This access is limited to what is necessary to carry out the support task.
- Data-related assistance — clients may send iCT4 data files, extracts, or reports and ask for help with formatting, importing, or analysing them. In these cases iCT4 handles the data solely for the purpose of providing the requested assistance and does not retain it beyond that task.

In all cases, iCT4 acts only on the instructions of the client and does not use client data for any purpose of its own.

Types of data we may have sight of

The personal data iCT4 engineers may encounter during service delivery depends on the client and the nature of the support. It is not data iCT4 collects or controls. It may include:

Education clients (schools, academies and multi-academy trusts)

- Pupil data: names, dates of birth, year group, attendance, assessment data, photographs
- Special educational needs and disabilities (SEND) data, including health and medical information — special category data requiring heightened protection
- Safeguarding and child protection records — special category data
- Staff data: names, job roles, contact details, payroll information, DBS status
- Parent and carer contact details
- Data held within school management information systems (MIS), email platforms, cloud environments (such as Microsoft 365), and network

www.ict4.co.uk hello@ict4.co.uk
01209 311344 Trevenson House, Church Road, Redruth, TR15 3PT

infrastructure. Where schools use online services provided or approved by the school for pupils, iCT4 will, where relevant to the service, ensure those services meet children's higher data protection requirements as set out in the DUAA 2025.

Business clients

- Employee and contractor contact details and HR records
- Customer and supplier data held in business systems
- Financial and accounting records
- Emails, files, and data held across network infrastructure, servers, and cloud platforms

Our obligations as a data processor

iCT4 meets its obligations as a data processor under Article 28 UK GDPR. All service delivery where personal data may be accessed is underpinned by a written Data Processing Agreement (DPA) agreed with the client. This is a legal requirement under Article 28. Our processor obligations include:

- Processing data only on documented instructions from the client and for no other purpose
- Maintaining Records of Processing Activities (RoPA) covering processing carried out on behalf of clients, as required by Article 30(2) UK GDPR
- Implementing appropriate technical and organisational security measures proportionate to the risk, in line with Article 32 UK GDPR
- Not engaging sub-processors unless they meet the same data protection standards required of iCT4 under UK GDPR. We carry out internal due diligence on all sub-processors before engagement and where arrangements change, we ensure the replacement meets equivalent standards. A current list of our principal sub-processors is available to clients on request.
- Notifying the client without undue delay — and in any event within 72 hours of becoming aware — of any personal data breach affecting their data, to enable the client to meet their own ICO notification obligations where required
- Assisting the client in responding to data subject rights requests, data protection impact assessments (DPIAs), and regulatory enquiries
- On termination of services, returning all client data in iCT4's possession and securely deleting any copies, unless retention is required by law
- Permitting and cooperating with audits or inspections by the client or their appointed auditor

Staff access to school systems

Engineers who access school systems may encounter data relating to children. iCT4 ensures that staff with access to school environments hold appropriate clearances, including Disclosure and Barring Service (DBS) checks where required, and are aware of their obligations under Keeping Children Safe in Education (KCSIE) guidance. Access to client systems is granted on a need-to-access basis and is logged and monitored.

Special category data

www.ict4.co.uk hello@ict4.co.uk
01209 311344 Trevenson House, Church Road, Redruth, TR15 3PT

Where iCT4 engineers have sight of special category data — including SEND, medical, safeguarding, or biometric data — in the course of providing support, we apply additional controls:

- Access is limited to authorised engineers on a strict need-to-access basis
- No special category data is copied, extracted, or retained beyond the immediate support task unless explicitly instructed by the client
- Sub-processors who may encounter special category data are subject to enhanced due diligence
- Any incident involving special category data is escalated immediately to the client's DPR or DPO

Data subjects' rights in the processor context

Where iCT4 is acting as a data processor, data subjects (pupils, staff, parents, employees) should direct rights requests — such as subject access or erasure requests — to the client organisation (the data controller) in the first instance. iCT4 will assist the client in fulfilling those requests within agreed timescales as set out in the Data Processing Agreement.

Part C: Provisions applying to both roles

Data security

We take data security seriously across all our activities. Our measures include:

- UK-based secure databases for client contact data, encrypted at rest and in transmission and accessible only over secure encrypted channels
- Multi-factor authentication (MFA) enforced on all systems that support it
- Company-owned devices encrypted, password-protected, and set to auto-wipe after a number of failed entry attempts
- Password policies aligned with NCSC guidance: strong passphrases, minimum 12 characters without MFA and minimum 8 with MFA
- Cyber Essentials certification and security policies aligned with DfE Digital Standards and NCSC guidance for MSPs supporting schools
- Documented procedures for managing actual or suspected data breaches, with notification to affected clients and the ICO where legally required
- Regular staff training on data protection obligations and information security

Data retention

We retain personal data only as long as necessary for the purpose for which it was collected, and in line with contractual, legal, and financial obligations. We maintain an internal data retention schedule covering all categories of data we hold. Data accessed in the course of providing support is not retained beyond the immediate task unless the client instructs us to do so. On termination of a client contract, client data in our possession is returned or securely deleted as agreed in the Data Processing Agreement.

Data sharing

We may share personal data with sub-contractors and service providers where necessary to deliver contracted services. All third parties are required to process data securely and only for the purpose for which it was shared. We may also share data where legally required, including with:

www.ict4.co.uk hello@ict4.co.uk
01209 311344 Trevenson House, Church Road, Redruth, TR15 3PT

- Government bodies and regulators, to meet legal obligations
- Financial institutions, for payment processing
- Law enforcement agencies, where required by law or to prevent or detect crime

In the event of a merger, acquisition or sale of iCT4 Limited, personal data may transfer to the relevant third party. We would inform you of any such change and your data would continue to be used as set out in this notice.

Transferring data internationally

Where personal data is transferred outside the UK, we ensure appropriate safeguards are in place in accordance with UK data protection law, including UK adequacy regulations, the UK Extension to the EU-US Data Privacy Framework, or standard contractual clauses approved under UK law. We do not transfer personal data internationally without a lawful basis.

Automated decision-making and profiling

We do not make decisions about individuals using solely automated processing, including profiling, that produce legal or similarly significant effects.

Your rights — client contacts

Where iCT4 acts as data controller for your contact data, you have the right to:

- Access the personal data we hold about you (subject access request)
- Have inaccurate or incomplete data corrected
- Have your data erased in certain circumstances
- Restrict the way we process your data in certain circumstances
- Receive your data in a portable format where processing is based on consent or contract and is carried out by automated means
- Object to our processing, including for direct marketing — we will always comply with an objection to direct marketing
- Not be subject to solely automated decision-making with significant effects on you
- Withdraw consent at any time where processing is based on consent
- Make a data protection complaint directly to us and, if unresolved, to the ICO

Making a subject access request

Please contact our DPR. You will be asked to provide suitable identification. If we hold information about you, we will provide a description of the data, why we hold it, where we obtained it from, who it has been shared with, and a copy in an intelligible form. We will respond within one calendar month. Where a request is complex, we may extend this by up to a further two months and will notify you within the first month. We will only conduct searches that are reasonable and proportionate in scope. If we need further information from you to process your request, we will pause the response period, notify you promptly, and resume it once we have what we need.

Complaints process

www.ict4.co.uk hello@ict4.co.uk
01209 311344 Trevenson House, Church Road, Redruth, TR15 3PT

You have a statutory right to raise a data protection complaint directly with us. You can do so by contacting any member of our team, telephoning our office, or writing to the DPR at the address in the Contact Us section below. We will acknowledge your complaint within 30 days and work to resolve it promptly.

If you remain dissatisfied, you can escalate to the Information Commissioner's Office (ICO), the UK's independent supervisory authority for data protection, sponsored by the Department for Science, Innovation and Technology (DSIT):

- Via their web form at: https://ico.org.uk/make-a-complaint/
- Via live chat on the ICO website
- By calling: 0303 123 1113
- In writing to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

For any questions about this notice or to exercise your rights, please contact our Data Protection Representative (DPR).

Data Protection Representative: Jonathan Jenkin | dpo@ict4.co.uk

www.ict4.co.uk
hello@ict4.co.uk
01209 311344
Trevenson House, Church Road, Redruth, TR15 3PT