Data Privacy Policy

Last policy review date:	06/01/2026
Reviewed by:	Farida Mirza
Policy publication/dissemination date:	January 2026
Next review due:	January 2027

Introduction

Community Systems is committed to protecting your privacy when you provide your personal information. This policy explains how we collect and use personal data, and how we protect your privacy. It also sets out your rights over your personal data and how to contact us and the supervisory authority.

Context and Applicable Law

Community Systems must collect and share personal information about employees and learners to perform tasks required by our business and by law. The core legislation is the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). From 19 June 2025, targeted reforms introduced by the Data (Use and Access) Act 2025 (DUAA) are being implemented in stages. These include updates to lawful bases, subject access requests, automated decision-making, international transfers and rules under the Privacy and Electronic Communications Regulations (PECR). We will continue to monitor commencement regulations and ICO guidance and align our practices as provisions take effect.

Data protection principles

Everyone responsible for using personal data must follow the data protection principles. Personal data must be: used fairly, lawfully and transparently; used for specified, explicit purposes; adequate, relevant and limited to what is necessary; accurate and, where necessary, kept up to date; kept no longer than necessary; and processed with appropriate security to protect against unauthorised or unlawful processing, access, loss, destruction or damage.

There is stronger legal protection for more sensitive information (special category data), such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetics, biometrics (for identification), health and sex life or orientation. Separate safeguards apply to data relating to criminal convictions and offences.

Who we are

Community Systems is a limited company (Company No. 2806784). Registered address: Ujima House, 388 High Rd, Wembley HA9 6AR. We provide government-funded accredited and non-accredited training for adults through subcontracting arrangements with other organisations.

For learner data submitted via the Individualised Learner Record (ILR), the Department for Education (DfE) acts as the data controller and Community Systems acts as a data processor for that submission. For other processing activities we undertake (e.g., enrolment, teaching, safeguarding, employer engagement), Community Systems will typically act as the data controller, determining the purposes and means of processing.

DfE uses learners' personal information to exercise its statutory functions (including creating and maintaining a unique learner number (ULN) and personal learning record (PLR)). See the DfE Personal Information Charter and ILR privacy notice for further details.

Contact

If you have any queries about this Policy, the way in which Community Systems processes personal data, or about exercising any of your rights, you can contact our Privacy Officer by sending an email to howard.thraves@communitysystems.co.uk or writing to Privacy Officer, Community Systems, Ujima House, 388 High Rd, Wembley HA9 6AR.

What personal data do we collect?

We collect personal data from employees and learners including name, address, gender, date of birth, telephone, email and residency information (e.g., passport/ID numbers, visa or Home Office documents). We also collect special category data where required (e.g., ethnicity, benefit status, health or learning difficulty/disability). This data is required under employment law and funding/quality rules to deliver our services and meet standards set by DfE, awarding bodies and regulators.

We may collect additional data to administer reasonable adjustments, specific qualifications or programmes, and for quality assurance, investigations, complaints or appeals.

How do we use your personal data?

We process personal data on the following lawful bases: public task (to perform tasks required by statute or funding rules), contract (to deliver employment or training services), legal obligation (to comply with law), and legitimate interests (for certain activities such as network and information security or internal administration, balanced against your rights).

We use data to: manage employment; claim/access funding; administer programmes; contact you about quality assurance, investigations, appeals and complaints; monitor performance; and communicate essential service updates. Electronic direct marketing will only be undertaken in compliance with PECR and where appropriate consent or "soft opt-in" rules apply.

Where/how do we keep sensitive data?

Data from forms is transferred to secure electronic storage or restricted-access file storage. Electronic data is kept on secure cloud infrastructure provided by certified organisations. We maintain effective security aligned to Cyber Essentials Plus and review controls annually. All staff follow our clean desk policy and use lockable storage for paperwork. Secure methods are used when transporting or posting sensitive paperwork.

Who do we share your personal data with?

We share personal data with relevant third parties where necessary to deliver employment, learning, assessment or certification, including: DfE and its executive agencies; funding bodies; partner organisations; awarding bodies; and other Government Departments (e.g., Department for Work and Pensions), in compliance with data protection law and applicable contracts. We may also share data if required by law (e.g., law enforcement, prevention of crime or fraud, or to protect life in an emergency).

International transfers

Where we transfer personal data outside the UK, we rely on appropriate safeguards under UK GDPR. For transfers to the United States, we may use the UK–US Data Bridge (the UK extension to the EU–US Data Privacy Framework) where the recipient is certified to the UK extension, or other mechanisms (e.g., IDTA/Addendum or Binding Corporate Rules). We document transfer assessments and update privacy information accordingly.

How long will we keep your personal data?

We retain personal data only for as long as necessary for the purposes collected. For ILR learner data, DfE retains operational data for up to 20 years and may retain personal data in research databases until age 80 for long-term research purposes. Other records follow our retention schedule based on contractual, legal, audit and regulatory requirements.

Your rights

You have rights to access, rectify, erase, object, restrict processing and data portability, subject to legal exceptions. Requests will be handled within one month; in complex cases we may extend by up to two months and, where reasonably necessary to clarify a request, we may pause ("stop the clock") while awaiting information. Searches will be reasonable and proportionate. You can also make complaints to us about our handling of your personal data.

Cookies and similar technologies

Our services use cookies and similar technologies in line with PECR. We obtain consent for non-essential cookies unless an exception applies. Following DUAA reforms, certain low-risk analytics or functionality cookies may be permitted without consent as commencement regulations take effect. We will update our cookie notices and consent tools accordingly.

Complaints

If we cannot resolve your concern, you can lodge a complaint with the UK Information Commissioner's Office (ICO): https://ico.org.uk/concerns/.

Changes to this policy

This policy is reviewed annually. We will notify material changes by email and publish updates on our website.