DCME SOFTWARE

Care Management Software

PRIVACY POLICY

Data Protection & GDPR Compliance

Version:	1.0
Effective Date:	12 April 2026
Next Review Date:	12 April 2027
Policy Owner:	DCME Software Ltd
Website:	https://dcmesoftware.services/

1. Introduction and Overview

DCME Software Ltd ("DCME", "we", "us", or "our") is committed to protecting and respecting the privacy of all individuals whose personal data we process. This Privacy Policy explains how we collect, use, store, share, and protect personal data in connection with the DCME care management software platform and the website available at https://dcmesoftware.services/ (together, the "Platform").

This Privacy Policy has been prepared in accordance with:

- The UK General Data Protection Regulation (UK GDPR) as retained in domestic law by the European Union (Withdrawal) Act 2018
- The Data Protection Act 2018 (DPA 2018)
- The Privacy and Electronic Communications Regulations 2003 (PECR)
- Guidance issued by the Information Commissioner's Office (ICO)
- The Care Quality Commission (CQC) standards and relevant health and social care legislation

By using the Platform, you acknowledge that you have read and understood this Privacy Policy. If you are using the Platform on behalf of an organisation (such as a care provider), you confirm that you have authority to bind that organisation to this Policy.

Important Notice for Special Category Data

DCME processes special category personal data (including health and medical information) on behalf of care providers. This is subject to enhanced legal protections under Article 9 of the UK

GDPR and Schedule 1 of the Data Protection Act 2018. We apply the highest standards of data protection to all such information.

2. Who We Are – Data Controller and Data Processor

2.1 Data Controller Identity

DCME Software Ltd acts as a Data Controller in respect of personal data collected through our website and as a Data Processor in respect of personal data processed within the care management software on behalf of our client organisations (care providers).

Company Name:	DCME Software Ltd
Website:	https://dcmesoftware.services/
Role:	Data Controller (website) / Data Processor (platform)
Regulatory Authority:	Information Commissioner's Office (ICO), United Kingdom
Contact:	enquiries@dcmesoftware.services

2.2 Data Processor Obligations

Where DCME acts as a Data Processor on behalf of care provider organisations (our clients, who are the Data Controllers), we process personal data only on the documented instructions of those clients. A Data Processing Agreement (DPA), compliant with Article 28 of the UK GDPR, is in place with each client organisation.

3. Personal Data We Collect

3.1 Service User Data

In connection with providing care management services, DCME processes the following categories of personal data relating to service users (care recipients):

3.1.1 Identifying Information

- Full name, date of birth, gender, and NHS number
- Home address and contact details
- Emergency contact names and relationships
- Photograph or image (where provided)

3.1.2 Special Category Health and Medical Data (Article 9 UK GDPR)

- Medical diagnoses, conditions, and clinical history
- Prescribed medications and dosage information
- Allergy and adverse drug reaction records
- Mental capacity assessments and best interest decisions
- Risk assessments and care needs assessments

- Detailed care and support plans
- Progress notes and daily appointment records
- Accident, incident, and safeguarding records
- Hospital admission and discharge information
- Fluid and food intake records
- Behavioural support plans

3.1.3 Financial and Administrative Data

- Local authority funding arrangements and reference numbers
- Commissioning and contract information
- Fee and invoice-related information (held by client organisations)

3.2 Staff and Carer Data

We process the following personal data relating to employees, contractors, and carers of our client organisations:

- Full name, job title, and employee or contractor reference number
- Contact details including work email address and telephone number
- Login credentials (securely hashed passwords)
- Working schedules, shift patterns, and rota information
- Training records, qualifications, and certifications
- DBS (Disclosure and Barring Service) check status and dates
- Supervision and appraisal records
- Absence and leave records
- System access logs and audit trail information

3.3 Website Visitor Data

When individuals visit https://dcmesoftware.services/, we may collect:

- IP address and browser type
- Pages visited, referral source, and time spent on site
- Device information
- Contact form submissions (name, email address, message content)
- Cookie data – see Section 10 of this Policy

4. Legal Basis for Processing

We only process personal data where we have a lawful basis under Article 6 of the UK GDPR. For special category data, we additionally rely on a condition under Article 9. The legal bases we rely upon are set out below.

Processing Activity	Article 6 Basis	Article 9 Basis (where applicable)
Care planning and delivery records for service users	6(1)(b) – necessary for contract / 6(1)(c) – legal obligation (Care Act 2014, Health & Social Care Act 2008)	9(2)(h) – health or social care provision
Medication administration records	6(1)(c) – legal obligation	9(2)(h) – provision of health care; Schedule 1 para 2 DPA 2018

Safeguarding records	6(1)(c) – legal obligation	9(2)(b) – employment / social protection law
Staff employment and HR records	6(1)(b) – employment contract; 6(1)(c) – legal obligation	9(2)(b) – where health data is held for occupational health
DBS check information	6(1)(c) – legal obligation	9(2)(b) – employment law – Schedule 1 DPA 2018
System audit logs and access records	6(1)(f) – legitimate interests (information security and accountability)	N/A
Website contact forms and enquiries	6(1)(a) – consent / 6(1)(b) – pre-contractual steps	N/A
Website analytics and cookies	6(1)(a) – consent (where required by PECR)	N/A

5. How We Use Personal Data

5.1 Service Users

Personal data relating to service users is processed to:

- Create and maintain accurate, individualised care plans
- Record and monitor the delivery of care and support
- Manage medication administration and health monitoring
- Facilitate safe and effective communication between care staff
- Meet statutory reporting and regulatory requirements under the Care Act 2014, Health and Social Care Act 2008, and CQC fundamental standards
- Respond to safeguarding concerns and record incidents
- Support transitions of care and multi-agency working

5.2 Staff and Carers

Personal data relating to staff is processed to:

- Manage employment and contractual obligations
- Allocate shifts, rotas, and care assignments
- Record training, competency, and qualifications
- Maintain DBS check compliance records
- Facilitate supervision, appraisal, and performance management
- Ensure accountability through system audit trails
- Comply with employment law obligations

5.3 Website Visitors and Enquirers

Data collected via the website is processed to:

- Respond to enquiries submitted via contact forms
- Provide information about DCME's products and services
- Improve website performance and user experience
- Comply with security and legal obligations

6. Sharing of Personal Data

6.1 General Principles

DCME does not sell, rent, or trade personal data. We only share personal data where there is a lawful basis to do so and where appropriate safeguards are in place.

6.2 Sharing by Client Organisations

Care provider organisations using the Platform may share service user or staff data with the following categories of recipients, subject to their own data protection obligations:

- NHS trusts, GPs, and other healthcare professionals involved in an individual's care
- Local authorities and commissioning bodies
- Regulatory bodies including the CQC and Ofsted
- Emergency services where there is a risk to life
- Third-party health and social care providers involved in a care package

6.3 DCME's Sub-Processors and Third Parties

DCME engages a limited number of carefully vetted sub-processors to support Platform delivery. All sub-processors are bound by data processing agreements that comply with Article 28 of the UK GDPR. Categories of sub-processors include:

- Cloud infrastructure and hosting providers Amazon AWS (within the UK or EEA).
- Cyber security and penetration testing services Alpha OBS LLP
- Technical support and software development partners operating under strict confidentiality obligations Alpha OBS LLP.
- Analytics providers Google (anonymised or pseudonymised data only).

6.4 Legal Disclosures

We may disclose personal data to law enforcement, regulatory authorities, or courts where required by law, or where necessary to protect the rights, property, or safety of DCME, our clients, or others.

7. International Data Transfers

DCME stores and processes all personal data within the United Kingdom or, where applicable, within the European Economic Area (EEA). We do not transfer personal data to third countries outside the UK or EEA except where:

- The transfer is to a country with a UK adequacy decision under Article 45 of the UK GDPR;
- Appropriate safeguards are in place, such as International Data Transfer Agreements (IDTAs) or UK Addendum to the EU Standard Contractual Clauses; or
- An exemption under Article 49 of the UK GDPR applies.

Any such transfers are subject to a Transfer Impact Assessment (TIA) to ensure equivalent protection is maintained. Where cloud services or sub-processors are located outside the UK, DCME ensures that contractual and technical safeguards are in place before any transfer occurs.

8. Data Retention

8.1 Retention Principles

We retain personal data only for as long as is necessary for the purposes for which it was collected, and in accordance with our legal obligations, regulatory requirements, and our clients' retention schedules.

8.2 Retention Schedule

Data Category	Minimum Retention Period	Legal Basis for Period
Service user care records	8 years post-discharge (adult)	NHS Records Management Code of Practice 2021; Care Act 2014
Child service user records	Until age 25 or 8 years post-discharge (whichever is later)	NHS Records Management Code of Practice 2021
Medication administration records	8 years	Care Act 2014; regulatory requirements
Incident and accident records	8 years	Limitation Act 1980; regulatory requirements
Safeguarding records	8 years minimum; indefinitely in some circumstances	Local safeguarding procedures; serious case review requirements
Staff employment records	6 years post-employment	Limitation Act 1980; employment law
DBS check records	6 months post-decision	DBS Code of Practice
System audit logs	3 years	Security and accountability requirements
Website contact data	2 years from last contact	Legitimate interests; PECR

Upon expiry of applicable retention periods, personal data is securely deleted or anonymised in accordance with our Secure Disposal Policy. In addition, where DCME processes personal data on behalf of a client organisation under a contractual arrangement, all personal data held in connection with that contract will be securely deleted or returned to the client upon expiry or termination of that contract, unless retention is required by law.

9. Your Rights as a Data Subject

Under the UK GDPR and Data Protection Act 2018, individuals have the following rights in relation to their personal data. These rights may be subject to exemptions in certain circumstances, including where data is processed for health and social care purposes.

Right	Description and Applicability
Right of Access (Article 15)	You have the right to request a copy of your personal data and supplementary information about how it is processed. We will respond within one calendar month.
Right to Rectification (Article 16)	You have the right to request correction of inaccurate or incomplete personal data without undue delay.
Right to Erasure (Article 17)	You may request deletion of your personal data where it is no longer necessary for the purpose it was collected, or where consent is withdrawn. Note: this right may not apply where retention is required by law or for public interest health purposes.

Right to Restrict Processing (Article 18)	You have the right to request that we restrict the processing of your data in certain circumstances, for example where accuracy is contested.
Right to Data Portability (Article 20)	Where processing is based on consent or contract, you may request your data in a structured, commonly used, machine-readable format.
Right to Object (Article 21)	You have the right to object to processing based on legitimate interests. This right is absolute where processing is for direct marketing purposes.
Rights in relation to Automated Decision-Making (Article 22)	DCME does not make solely automated decisions that produce legal or similarly significant effects without human involvement.
Right to Withdraw Consent	Where processing is based on consent, you may withdraw consent at any time without affecting the lawfulness of prior processing.

To exercise any of these rights, please contact us at enquiries@dcmesoftware.services. Where DCME processes data on behalf of a client organisation, requests should in the first instance be directed to that organisation as Data Controller. We will co-operate with requests in line with our obligations under Article 28(3)(e) of the UK GDPR.

10. Cookies and Tracking Technologies

Our website at https://dcmesoftware.services/ uses cookies and similar tracking technologies in accordance with the Privacy and Electronic Communications Regulations 2003 (PECR). We only place non-essential cookies with your prior consent.

10.1 Types of Cookies We Use

- Strictly Necessary Cookies: Essential for the website to function. These cannot be disabled.
- Performance and Analytics Cookies: Help us understand how visitors interact with our website (e.g., pages visited, errors encountered). Set only with your consent.
- Functional Cookies: Enable enhanced functionality such as remembering preferences. Set only with your consent.
- Marketing Cookies: DCME uses social media and marketing cookies on our website, including cookies set by Facebook, Google Analytics, Instagram, and TikTok. These cookies may track your browsing activity across websites to enable targeted advertising and to measure the effectiveness of our marketing campaigns. These cookies are only placed with your prior consent, in accordance with PECR.

10.2 Managing Cookies

You can manage cookie preferences at any time via our cookie consent tool on the website. You may also configure your browser to refuse cookies, though this may impair website functionality. For further information, visit www.allaboutcookies.org or the ICO's guidance on cookies.

10.3 Third-Party Social Media Platforms and Marketing Technologies

We use of social media and marketing technologies operated by third-party platforms, including Facebook (Meta), Google Analytics, Instagram, and TikTok. When you visit our social media accounts and have consented to marketing cookies, these platforms may collect data about your visit and use that data in accordance with their own privacy policies and terms of service.

Important Notice: DCME does not control how personal data collected via these third-party platforms is subsequently used, stored, or shared by those platforms. Each third-party provider acts as an independent data controller in respect of data they collect through their own technologies. We encourage you to review the privacy policies of the relevant platforms directly:

Facebook (Meta) Privacy Policy: https://www.facebook.com/privacy/policy

Google Analytics Privacy Policy: https://policies.google.com/privacy
Instagram (Meta) Privacy Policy: https://privacycenter.instagram.com/policy
TikTok Privacy Policy: https://www.tiktok.com/legal/page/eea/privacy-policy

11. Information Security

DCME implements comprehensive technical and organisational measures (TOMs) to protect personal data against accidental loss, destruction, alteration, unauthorised disclosure, or access, in accordance with Article 32 of the UK GDPR. These measures include:

11.1 Technical Measures

- End-to-end encryption of data in transit using TLS 1.2 or higher
- Encryption of personal data at rest using AES-256 or equivalent
- Multi-factor authentication (MFA) for all system access
- Role-based access controls (RBAC) limiting access to the minimum necessary
- Regular automated backups with tested recovery procedures
- Intrusion detection and prevention systems
- Regular penetration testing and vulnerability assessments
- Web application firewall (WAF) protection

11.2 Organisational Measures

- Mandatory data protection training for all staff with access to the Platform
- Documented information security policies and procedures
- Confidentiality agreements for all employees and contractors
- Regular data protection impact assessments (DPIAs) for high-risk processing activities
- Incident response and breach notification procedures
- Supplier due diligence and sub-processor management

12. Personal Data Breaches

In the event of a personal data breach, DCME will act in accordance with Articles 33 and 34 of the UK GDPR:

- We will assess and contain the breach without undue delay upon becoming aware of it.
- Where the breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the ICO within 72 hours of becoming aware of it.
- Where the breach is likely to result in a high risk to individuals, we will notify affected individuals directly without undue delay.
- We will document all breaches, including those that are not notifiable, and maintain a breach register.

Where DCME identifies a breach relating to data processed on behalf of a client organisation, we will notify that client without undue delay in accordance with our contractual obligations and Article 33(2) of the UK GDPR.

13. Data Protection Officer and Contact

DCME has appointed a Data Protection Officer (DPO) responsible for overseeing compliance with this Policy and with applicable data protection legislation.

> **Data Protection Contact**
> For any data protection queries, subject access requests, or to report a concern, please contact:Email: enquiries@dcmesoftware.servicesWebsite: https://dcmesoftware.services/We aim to respond to all requests within 5 working days and will resolve subject access requests within one calendar month.

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at any time:

- ICO Website: www.ico.org.uk
- ICO Helpline: 0303 123 1113
- ICO Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

14. Data Protection Impact Assessments

DCME conducts Data Protection Impact Assessments (DPIAs) in accordance with Article 35 of the UK GDPR before undertaking any processing that is likely to result in a high risk to the rights and freedoms of individuals. Given that DCME processes special category health data, DPIAs are carried out:

- Prior to the implementation of new features or processing activities involving special category data
- When deploying new technologies that may affect privacy
- When undertaking large-scale processing of sensitive personal data
- Where systematic monitoring of individuals is proposed

DPIA records are maintained and reviewed regularly. Where processing presents a high residual risk, DCME will consult the ICO prior to commencing processing.

15. Children's Data

The Platform may be used to record and manage care for children and young people under the age of 18. Such data constitutes special category data and is afforded the highest level of protection. DCME requires client organisations to:

- Ensure appropriate consents or legal bases are in place for processing children's data
- Apply enhanced access restrictions to records relating to children
- Comply with any court orders, care orders, or parental responsibility arrangements that affect data access and sharing

DCME's Platform is not designed for direct use by children under 18, and we do not knowingly collect data directly from children via our website.

16. Changes to This Privacy Policy

We review and update this Privacy Policy at least annually, or whenever there are significant changes to our processing activities, applicable legislation, or regulatory guidance. Material changes will be communicated to client organisations and, where applicable, notified on our website.

The most recent version of this Policy will always be available at https://dcmesoftware.services/. The effective date at the top of this document indicates when this version came into force. Continued use of the Platform following notification of changes constitutes acceptance of the revised Policy.

17. Glossary of Key Terms

Term	Definition
Data Controller	The organisation that determines the purposes and means of processing personal data.
Data Processor	An organisation that processes personal data on behalf of a Data Controller.
Data Subject	The individual to whom personal data relates.
Personal Data	Any information relating to an identified or identifiable living individual.
Special Category Data	Sensitive personal data including data concerning health, racial/ethnic origin, genetic data, biometric data, and other categories defined in Article 9 UK GDPR.
Processing	Any operation performed on personal data, including collection, storage, use, disclosure, or deletion.
UK GDPR	The UK General Data Protection Regulation, as retained in UK domestic law by the European Union (Withdrawal) Act 2018.
DPA 2018	The Data Protection Act 2018.
ICO	The Information Commissioner's Office – the UK's independent data protection authority.
DPIA	Data Protection Impact Assessment – a process to identify and mitigate privacy risks of new processing activities.
Sub-processor	A third party engaged by a Data Processor to process personal data on behalf of the Data Controller.

DCME SOFTWARE LTD

https://dcmesoftware.services/

enquiries@dcmesoftware.services

Policy Version 1.0 – Effective 12 April 2026