DATA PROTECTION POLICY

Contents

coolcare
admin made easy

T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

1. Policy statement

1.1. CoolCare Limited registered in England and Wales with company number 03462441 and whose registered office is at Helios 47, 1 Isabella Road, Garforth, Leeds, West Yorkshire, United Kingdom, LS25 2DY collectively referred to as “CoolCare”, “we”, “us”, “our”). CoolCare is registered with the Information Commissioners Office, under registration reference Z2293266. Everyone has rights with regard to the way in which their Personal Data in handled. During the course of our activities we will collect, store and Process Personal Data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2. This Data Protection Policy applies to all Personnel (“**you**”, “**your**”). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for us to comply with applicable law (although we understand that not all sections of this policy may be relevant to all Personnel, you should make sure you read and understand all of this policy). Your compliance with this Data Protection Policy is mandatory.. Any failure to comply puts both you and CoolCare at risk.

2. About this policy

2.1. The types of Personal Data that CoolCare may be required to handle includes information about current, past and prospective customers, business contacts, employees, staff, contractors, other individuals and others that we communicate with. The Personal Data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025 (‘Data Protection Legislation’)(together the “**Data Protection Legislation**”) and other regulations. This policy reflects changes introduced by the Data (Use and Access) Act 2025, which updates elements of the UK GDPR and Data Protection Act 2018.

2.2. This policy and any other documents referred to in it set out the basis on which we will Process any Personal Data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3. This policy does not form part of any employee's contract of employment and may be amended at any time. We do, however, require all staff to comply with it.

2.4. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, Process, transfer and store Personal Data.

2.5. CoolCare has nominated a Data Protection Officer contactable at dataprotection@lntgroup.co.uk who is responsible for ensuring compliance with the Data Protection Legislation and with this policy. That post is currently held by Jonathan Wharam. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to your line manager and the Data Protection Officer . The Data Protection Officer is responsible for:

a) keeping the organisation updated about data protection responsibilities, risks and issues;
b) reviewing data protection procedures and policies on a regular basis;
c) arranging data protection training and advice for staff members;
d) answering questions on data protection from other members of the organisation;
e) responding to individuals such as clients and employees who wish to know which data is being held on them by us; and
f) checking and approving with third parties that handle the company’s data any contracts or agreement regarding data Processing.

3. Definition of data protection terms

3.1. Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual for example our live chat on our website. Data Protection Laws prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

3.2. Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

3.3. Consent means an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject’s wishes by which they, by a statement or by clear positive action, signifies agreement to the Processing of Personal Data relating to them.

3.4. Data is information which is stored electronically, on a computer, or in certain paper-based filing systems;

coolcare
admin made easy

T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

3.5. Data Subject means a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

3.6. Data Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is Processed. They are responsible for establishing practices and policies in line with the Data Protection Legislation. We are the data controller of all Personal Data used in our business for our own commercial purposes;

3.7. Data Processors include any person or organisation that Processes Personal Data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle Personal Data on CoolCare's behalf;

3.8. Explicit Consent means consent which requires a very clear and specific statement, and is not just an action.

3.9. Personal Data means any information identifying at Data Subject or information relating to Data Subject that we can identify (directly or indirectly) from that data alone. Identifiers can include an identification name, location data or online identification or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. Personal Data includes Special Category Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

3.10. Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it, for example:

a) loss or theft of data or equipment on which personal information is stored;
b) unauthorised access to or use of personal information either by a member of staff or third party;
c) loss of data resulting from an equipment or systems (including hardware and software) failure;
d) human error, such as accidental deletion or alteration of data or sending data to the wrong person;
e) unforeseen circumstances, such as a fire or flood; deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
f) 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

3.11. Personnel: all employees, workers, contractors, agency workers, consultants, partners, directors and others.

3.12. Process, Processing or Processed, is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties;

3.13. Special Category Personal Data, or special categories of data include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special Category Personal Data can only be Processed under strict conditions, including a condition requiring the express permission of the person concerned; and

3.14. Supervisory Authority means the Information Commissioner's Office, subsequently to be known as the Information Commission or other relevant supervisory authority.

4. Data protection principles

4.1. Anyone Processing Personal Data must comply with the following principles of good practice. These provide that Personal Data must be:

a) Processed fairly, lawfully and in a transparent manner;
b) Processed for specified, explicit and legitimate purposes and in an appropriate way;
c) adequate, relevant and limited to what is necessary for the purpose;
d) accurate and kept up to date;
e) not kept longer than necessary for the purpose; and
f) Processed in line with data subjects' rights including in respect of the security of Personal Data.

We will also ensure Processing complies with any updated definitions and safeguards introduced under the Data (Use and Access) Act 2025 including specific provisions for Automated Decision Making and legitimate interests.

5. Fair and lawful Processing

5.1. The Data Protection Legislation is not intended to prevent the Processing of Personal Data, but to ensure that it is done fairly and lawfully in accordance with the rights of the data subjects.

5.2. For Personal Data to be Processed lawfully, they must be Processed on the basis of one of the legal grounds set out in the Data Protection Legislation. These include, among other things, the data subject's consent to

coolcare
admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

the Processing, or that the Processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed.. When Processing Personal Data as data controllers in the course of our business, we will ensure that those requirements are met and ensure that all staff who are responsible for Processing Personal Data will be aware of the conditions for Processing. It is important that you comply with this policy at all times and notify your line manager or the Data Protection Officer if you have any queries. Consent to Processing can be revoked at any time.

5.3. Processing may also be carried out under the "Recognised Legitimate Interests" lawful basis, as introduced by the Data (Use and Access) Act 2025. This includes Processing for crime prevention, safeguarding, responding to emergencies and other defined purposes. Where we rely on this basis, we will document our justification and ensure appropriate safeguards are in place.

5.4. CoolCare will need to Process Special Category Personal Data (such as if a customer makes a data subject request and provides their passport as a proof of identity). We will only Process Special Category Personal Data if:

a) we have a lawful basis for doing so as set out in paragraph 5.2 above; **and**

5.4.a.1.1. the data subject has given Explicit Consent;

5.4.a.1.2. the Processing is necessary for the purposes of exercising the employment law rights or obligations of CoolCare or the data subject;

5.4.a.1.3. the Processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving Consent;

5.4.a.1.4. Processing relates to Personal Data which are manifestly made public by the data subject;

5.4.a.1.5. the Processing is necessary for the establishment, exercise or defence of legal claims; or

5.4.a.1.6. the Processing is necessary for reasons of substantial public interest.

b) Before Processing any Special Category Personal Data, Personnel must notify the Data Protection Officer of the proposed Processing, so that they can assess whether the Processing complies with the criteria noted above.

c) Special Category Data will not be Processed until:

5.4.c.1. the assessment referred to in paragraph 5.4b) has taken place; and

5.4.c.2. the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the Processing, the purposes for which it is being carried out and the legal basis for it.

6. Consent

6.1. A data subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

6.2. Data subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the data subject first consented.

6.3. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category Personal Data , and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to Process most types of Special Category Personal Data. Where Explicit Consent is required, you must issue a fair Processing notice to the Data Subject to capture Explicit Consent.

6.4. You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

7. Processing for limited purposes

7.1. In the course of our business, we may collect and Process Personal Data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2. We will only Process personal data for the specific purposes for which we have obtained consent or otherwise have a basis for Processing in accordance with the Data Protection Legislation. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

8. Notifying data subjects

8.1. If we collect Personal Data directly from data subjects, we will inform them about:
- a) who is collecting the Personal Data and how it is being collected;
- b) the purposes for which we intend to Process that Personal Data;
- c) the types of third parties, if any, with which we will share or to which we will disclose that Personal Data;
- d) identity and contact details of any data controllers;
- e) details of transfers to other countries and safeguards;
- f) the retention period; and
- g) the means with which data subjects can limit our use and disclosure of their Personal Data, and any other rights they have in respect of the data.

8.2. If we receive Personal Data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

8.3. We will also inform data subjects whose Personal Data we Process that we are the data controller with regard to that data, and who the Data Protection Officer is.

8.4. Where data is used in Automated Decision-Making with legal or similarly significant effects, data subjects will be informed of this and of the right to obtain human intervention, express their view, or contest the decision.

9. Adequate, relevant and non-excessive Processing

9.1. We will only collect Personal Data to the extent that it is required for the specific purpose notified to the data subject.

9.2. We will keep full and accurate records of all our data Processing activities, including records of data subjects' consents and procedures for obtaining consents.

10. Accurate data

10.1. We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data. It must be corrected or deleted without delay when inaccurate.

10.2. Individuals may ask that we correct inaccurate Personal Data that we hold relating to them. If you believe that any data we hold is inaccurate, you should notify your line manager and the Data Protection Officer.

11. Timely processing

11.1. We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will maintain a retention policy and procedure and take all reasonable steps to ensure that we destroy, or erase from our systems, all data which is no longer required.

12. Processing in line with data subject's rights

12.1. We will Process all Personal Data in line with data subjects' rights, in particular their right to: Data Subjects have rights when it comes to how we handle their Personal Data, and can exercise these rights at any time. These include rights to:

a) to be informed about how, why and on what basis their Personal Data is being Processed, for example a privacy notice:

b) withdraw Consent to Processing at any time;

c) request access to their Personal Data that we hold;

d) prevent our use of their Personal Data for direct marketing purposes;

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

f) restrict Processing in specific circumstances;

coolcare
admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

i) object to decisions based solely on Automated Processing, including profiling (ADM);

j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

l) make a complaint to the Supervisory Authority; and

m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

These rights are detailed further in paragraph 20 onwards.

13. Data security

13.1. We will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. We will regularly evaluate the effectiveness of these measures to ensure security of our Processing pf Personal Data. You must exercise particular care in protecting sensitive Personal Data from loss and unauthorised access, use or disclosure.

13.2. We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a data Processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself.

13.3. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) confidentiality means that only people who are authorised to use the data can access it;
b) integrity means that personal data should be accurate and suitable for the purpose for which it is Processed; and
c) availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

13.4. Security procedures include:

a) entry controls. Any stranger seen in entry-controlled areas should be reported;
b) secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential);
c) methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required; and
d) equipment. Personnel must ensure that individual monitors do not show confidential information to passers-by and that they lock/log off from their computer/mobile phone when it is left unattended.
e) Devices. All PCs, Laptops and Mobiles must be password protected.

13.5. We are required to comply with obligations under Data Protection Legislation where we use third parties to Process Personal Data on our behalf (including but not limited to IT software providers and HR payroll providers). In these circumstances, such parties will be acting as our Data Processor and Data Protection Legislation requires us to put in place a contract in writing which contains a number of provisions to help safeguard the Personal Data. If you are responsible for the drafting or negotiation of contracts with Data Processors, you must seek further advice from the Data Protection Officer to ensure the contracts contain all the necessary data protection provisions.

13.6. Where we share Personal Data with third parties for their own use (and they will not be Processing data on our behalf) it will often be necessary to enter into a data sharing agreement. We need to ensure that such agreements contain certain provisions such as the third party will only Process the Personal Data for specific purposes, to return the Personal Data to us in certain circumstances and have adequate security measures in place. If you are required to enter into a data sharing agreement, you must seek further advice from the Data Protection Officer.

13.7. In all cases, we may only share the Personal Data we hold provided the sharing complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.

coolcare
admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

14. Transferring Personal Data to a country outside the United Kingdom (Restricted Transfers)

14.1. Data Protection Legislation restrict transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by Data Protection Legislation is not undermined. We may transfer any Personal Data we hold to a country outside the United Kingdom only after discussing it further with the Data Protection Officer and provided that one of the following conditions applies:

a) the UK Government has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms, please see the ICO's website for details of those countries, ;

b) the data subject has given their Explicit Consent to the proposed transfer after being informed or any potential risks; or

c) the transfer is necessary for one of the other reasons set out in Data Protection Legislation including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

14.2. Subject to the requirements in clause 14.1 above, Personal Data we hold may also be Processed by staff operating outside the United Kingdom who work for us or for one of our suppliers. These staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the Processing of payment details and the provision of support services.

15. Accountability

15.1. The Data Controller (CoolCare) must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

a) We must have adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including:

15.1.a.1. appointing a suitably qualified Data Protection Officer (where necessary) where the appointment of a Data Protection Officer is not a legal requirement, we must still appoint an individual/individuals with responsibility for overseeing our compliance with Data Protection Legislation such as a Data Protection Officer;

15.1.a.2. implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

15.1.a.3. integrating data protection into internal documents including this Data Protection Policy, related policies and privacy notices;

15.1.a.4. regularly training Personnel on Data Protection Legislation, this Data Protection Policy, related policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. We must maintain a record of training attendance by Personnel; and

15.1.a.5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

15.2. **Record Keeping**

a) Data Protection Legislation requires us to keep full and accurate records of all our data Processing activities.

b) You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents.

c) We must also keep records of the name and contact details of the Data Controller and the Data Protection Lead, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data transfers outside the UK and the safeguards put in place to protect the transfer of such Personal Data, the Personal Data's retention period and a description of the security measures in place.

coolcare
admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

d) If we Process Special Category Personal Data and criminal records information, we will also keep written records of:

15.2.d.1. the relevant purpose for which the Processing takes place, including (where required) why it is necessary for that purpose;

15.2.d.2. the lawful basis for our Processing; and

15.2.d.3. whether we retain and erase the Personal Data in accordance with our policy document and, if not, the reasons for not following our policy.

e) Our data Processing records must always be kept up to date. Please see ICO guidance for further details regarding the information we must record: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

f) We will conduct regular reviews of the Personal Data we Process and update our documentation according. This may include:

15.2.f.1. carrying out information audits to find out what Personal Data CoolCare holds;

15.2.f.2. distributing questionnaires and talking to Personnel across CoolCare to get a more complete picture of our Processing activities; and/or

15.2.f.3. reviewing our policies, procedures, contract and agreements to address areas such as retention, security and data sharing.

15.3. **Training And Audit**

a) We are required to ensure all Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and Processes to assess compliance.

b) You must regularly review all the systems and Processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

16. Data Protection Impact Assessment (DPIA)

16.1. We will implement appropriate technical and organisational measures to ensure compliance with data privacy principles taking into consideration the nature, scope, context and purposes of Processing and the risks of varying likelihood and severity for the rights and freedoms of data subjects posed by the Processing.

16.2. We will conduct DPIAs in respect to high-risk Processing. DPIAs should be carried out and discussed with the Data Protection Officer when implementing major system or business change programs involving the Processing of Personal Data including:

a) use of new or changing technologies (programs, systems or Processes) or changing technologies;
b) large scale Processing of sensitive Personal Data; and
c) large scale, systematic monitoring of a publicly accessible area.
d) DPIAs will also be completed where new technologies involve Automated Decision Making, biometric or facial recognition data, or large-scale employee monitoring.

16.3. The DPIA must include:

a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
c) an assessment of the risk to individuals; and
d) the risk mitigation measures in place and demonstration of compliance.

15.4 Where research, innovation or children's data Processing is undertaken, we will apply additional safeguards introduced by the Data (use and Access) Act 2025.

coolcare admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

17. Automated Processing (Including Profiling) and Automated Decision Making

17.1.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

17.1.1.1 a Data Subject has Explicitly Consented;

17.1.1.2 the Processing is authorised by law; or

17.1.1.3 the Processing is necessary for the performance of or entering into a contract.

17.1.2 If certain types of Special Category Personal Data are being Processed, then grounds 17.1.1.2 or 17.1.1.3 will not be allowed but such Special Category Personal Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

17.1.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object.

17.1.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

17.1.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken which have a legal effect or similar significant effect on the Data Subject. Note that not all Automated Processing will have a legal or similar effect on a Data Subject, for example, targeted advertising is generally not considered to have a significant effect on individuals.

18. Disclosure and sharing of personal information

18.1. We may share Personal Data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

18.2. You may only share Personal Data we hold with another employee, agent or representative of CoolCare if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

18.3. We may also disclose Personal Data we hold to third parties:

a) if sharing the Personal Data complies with our privacy policy and, if required, the data subject's consent has been obtained;
b) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
c) we have a written contract in place with the third party which contains GDPR approved third party clauses;
d) if we sell or buy any business or assets, in which case we may disclose Personal Data we hold to the prospective seller or buyer of such business or assets; or
e) if we or substantially all of our assets are acquired by a third party, in which case Personal Data we hold will be one of the transferred assets; or
f) if we are under a duty to disclose or share a data subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or
g) to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

19. Dealing with subject access requests

19.1. Data subjects may make a formal request for information we hold about them free of charge. This should be made in writing addressed to the Data Protection Officer although a data subject is entitled to make the request to any member of staff. The request may be made in writing by any means, including email, fax or via a web enquiry. Employees who receive a written request or think they may have received a request should forward it to their line manager and Data Protection Officer immediately.

coolcare
admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

19.2. When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:
   a) we will check the caller's identity to make sure that information is only given to a person who is entitled to it; and
   b) we will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

19.3. Subject to the provision of limited information in accordance with clause 19.2 above, Personnel should not respond to a subject access request without first discussing the request with their line manager/the Data Protection Officer . Please note that there are strict requirements placed on all organisations in respect of dealing with and responding to subject access requests. Any failure of CoolCare in this respect could result in significant fines and other penalties being imposed on CoolCare. It is therefore important that you immediately notify your line manager and the Data Protection Officer of any subject access request. In line with the Data (Use and Access) Act 2025, we have a duty to conduct searches on a reasonable and proportionate basis and the one-month time limit for responding may be paused ("stop the clock") while we seek clarification from the requester where necessary to identify the data requested.

20. Data portability

20.1. Data subjects have the right to receive a copy of their data in a structured format and for their data to be transferred directly to another system, free of charge. Any such request should be Processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. If you need further information, please contact your line manager or the Data Protection Officer. .

21. Right to be forgotten

21.1. Data subjects have the right to request that any information held on them is deleted or removed, and any third parties who Process or use that data must also comply with such request. This type of request can only be refused if an exemption applies. The Data Protection Officer will make the final decision.

22. Requests made by a data subject in respect of their rights

22.1. Any requests made by a data subject in relation to any of the rights which they have in relation to their Personal Data should be referred to the Data Protection Officer as soon as possible to ensure that such requests are dealt with in a timely and appropriate manner.

23. Reporting breaches

23.1. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:
   a) investigate the failure and take remedial steps if necessary;
   b) maintain a register of compliance failures; and
   c) notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures.

23.2. Please report any failures to your line manager and the Data Protection Officer without undue delay. Please note that there are strict requirements placed on all organisations in respect of reporting a breach to the Supervisory Authority. Any failure of CoolCare in this respect could result in significant fines and other penalties being imposed on CoolCare. It is therefore important that you immediately notify your line manager and the Data Protection Officer of any breach or suspected breach. We will also record and investigate all personal data breaches, whether or not they are reportable to the ICO, in accordance with the updated ICO guidance issued under the Data (Use and Access) Act 2025.

23.3. Where we act as a Data Processor for a third party, please report any failures to your line manager and the Data Protection Officer without undue delay. The Data Protection Officer will liaise with you accordingly to ensure that the Data Controller is made aware of the Personal Data Breach.

24. Monitoring

24.1. Everyone must observe this policy. The Data Protection Officer has overall responsibility for this policy. Monitoring of staff, systems or communications will only be carried out where lawful, necessary and proportionate, and subject to a Data Protection Impact Assessment where required by ICO guidance on employment practices.

25. Changes to this policy

25.1. We reserve the right to supplement or amend this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email. Any new or modified policy will be circulated to staff.

25.2. This Data Protection Policy does not override any applicable national Data Protection Legislation.

26. Contact/Information

26.1. If you have any queries or require any further assistance or information in relation to any of the contents of this policy, please contact Jonathan Wharam – Data Protection Officer at dataprotection@lntgroup.co.uk. Individuals can also submit data protection complaints electronically via dataprotection@lntgroup.co.uk. All complaints will be acknowledged, investigated and outcomes communicated in line with ICO expectations

Date reviewed: 20.10.25
Reviewer: Fiona Allen, Operations Director

Date	Created/Reviewed By	Comments/Updates Made
12.19	Fiona Hale	Reviewed, no updates made.
04.22	Fiona Hale	Updated DPO to Jonathan Wharam
08.23	Fiona Allen	Reviewed, no changes made
08.24	Fiona Allen	Reviewed on audit, no changes made
10.25	Fiona Allen	Reviewed on audit, updated to reflect changes following Data (Use and Access) Act 2025 (Clauses5.3, 17.3, 8.4,12,14,15.4, 24)

T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk