Cornwall Marine Network Ltd

Data Protection Policy

1 Overview

1.1 This policy provides guidance on how Cornwall Marine Network Ltd. and its associated companies (CMN) will process information about you, and explains your rights to access the information we hold for any individuals.

1.2 This policy applies to all individuals (current and former employees, workers, volunteers, apprentices, contractors, consultants and learners). If you fall into one of these categories, then you are a **'data subject'** for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data. It does not form part of your contract of employment, which can be amended at any time.

1.3 This policy was originally published to cover the requirements of the **General Data Protection Regulation 2022 (GDPR).**

1.4 As the EU GDPR does not apply in the UK after the end of the Brexit transition period on 31 December 2020. The EU GDPR is an EU Regulation and it no longer applies to the UK. As CMN operates inside the UK, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. CMN must comply with the both the **UK General Data Protection Regulation** and the **Data Protection Act 2018 (DPA 2018)**.

2 The key terms within Data Protection Legislation

2.1 The **Data Protection Act 2018 (the Act)**, is designed to protect people against misuse of their personal data held in both electronic and manual files. The Act is a complex piece of legislation and gives rights to individuals and lays down standards for the processing of personal data.

3 We refer to a number of terms throughout this policy

3.1. Data Controller

This is a person or group of people who determine how and why personal data is, or will be, processed. Senior management will nominate Data Controller(s) depending on the data being collected and then how it is manipulated. There can be a number of document controllers all taking control of how and who has access to the data that they require in their daily duties.

In the event that CMN are not the Lead partner for any contracts, CMN's role as data controller or processer might vary in line with contractual requirements, in such cases CMN would follow the Data Protection guidelines set out by the lead partner. The Project Managers would be responsible to ensure that all staff working on such contracts would be made aware of the differences, actions needed and implications of these changes.

3.2. Data Processor

A data processor is the one who carries out the actual processing of the data under the specific instructions of the data controller.

3.3. Data Subject

The living individual to whom the data relates.

3.4. Relevant Filing System

Any system where files are structured or referenced so that they clearly indicate whether they hold specific information which would amount to personal data.

3.5. Personal Data

Information from which a living individual can be identified (or can be identified from that data and other information in our possession)

3.6. Processing

Obtaining, capturing, recording, or holding the information or data or carrying out any operation on the information or data.

3.7. Sensitive or Special Categories of Data

Information relating to racial or ethnic origin, political opinions, religious or other beliefs, sex life, sexual orientation, trade union membership, biometric data, health and criminal convictions.

3.8. Source

The source of the personal data (e.g. application forms, payroll)

3.9. Disclosure

This occurs when data is passed by the data controller to an authorised third party.

3.10. CEO (Chief Executive Officer)

CMN's CEO is ultimately responsible for CMN's data protection policy and its implementation

3.11. Data Protection Officer

CMN Marketing and Events Coordinator is CMN's Interim DPO and can be contacted at dean.hodge@cornwallmarine.net

3.12. CMN takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

3.13 CMN has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject.

3.14 CMN has measures in place to protect the security of your data in accordance with our ICT Policy. A copy of this can be obtained from your line manager and can be found within CMN's Policy Manual / Handbook.

3.15 Nominated individuals within CMN are '**data controllers**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

3.16 This policy explains how CMN will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, CMN.

3.17 It is intended that this policy is fully compliant with the 2018 Act. If any conflict arises between those laws and this policy, CMN intends to comply with the 2018 Act.

4 Data Protection Principles

4.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

1) be processed fairly, lawfully and transparently;
2) be collected and processed only for specified, explicit and legitimate purposes;
3) be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
4) be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
5) not be kept for longer than is necessary for the purposes for which it is processed; and
6) be processed securely.

CMN is accountable for these principles and must be able to show that it is compliant.

5 How we define personal data

5.1 **'Personal data'** means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

5.2 This policy applies to all personal data whether it is stored electronically, on paper or on other Media.

5.3 This personal data might be provided to us by you, a third party (such as a former employer or your doctor) or generated by CMN. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or nominated personnel in the line of their duties.

6 Examples of Personal Data processed by CMN

6.1 Listed below are examples of personal data that CMN may hold about you. This is not an exhaustive list, and CMN may process other forms of data:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings)
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video); and
- any other category of personal data which we may notify you of from time to time.

7 How we define special categories of personal data

7.1 **'Special categories of personal data'** are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;

- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

8 How we define processing

8.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, capturing, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

9 Security of processing

9.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

9.2 In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

9.3 Adherence to an approved code of conduct as or an approved certification mechanism a may be used as an element by which to demonstrate compliance with the requirements set out in this policy.

9.4 The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by UK law.

10 How CMN will process your personal data

10.1 CMN will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act. We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else).

10.2 However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 16 below.

10.3 We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

10.4 If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

11 Examples of when we might process your personal data

CMN has to process personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example, (and see section below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;

- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of CMN, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend CMN in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and
- for any other reason which we may notify you of from time to time.

11.2 We will only process special categories of your personal data (refer to 7.1) in certain situations in accordance with the law. Prior to the processing of any special data, CMN would always consult you on the process and what the special category of data is being used for. You do not need to consent and can withdraw consent later if you choose by contacting your line manager.

11.3 CMN do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- processing relates to personal data which are manifestly made public by the person (data subject);
- where processing is necessary for the establishment, exercise or defence of legal claims; and

- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

11.4 We might process special categories of your personal data for the purposes in the section above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

11.5 There may be limited circumstances when we may make automated decisions about you using your personal data or use profiling in relation to you. For example, in the process of recruitment and selection processes (this will be in line with any legal obligations including but not limited to the Equality and Diversity, and the Disability Discrimination Act), and absence monitoring systems using biometric data entry systems.

12 Sharing your personal data

12.1 Sometimes CMN might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. These people are often known as 'processors'. This may include pension providers, payroll services, consultants such as HR, employee relation schemes and in some cases medical providers. The data processors are CMN employees, they may pass on specific information, under guidance from the Data Controller to a third party, for the reasons mentioned above. However, those third parties must be GDPR compliant, if not CMN can be liable for any fines for data breaches of the third party.

12.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

12.3 CMN will not send any personal data outside the UK. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

13How long will we keep your personal or sensitive data

13.1 CMN will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from the PA to CEO and Claims & Administration Manager.

14How should you process personal data for CMN

14.1 Everyone who works for, or on behalf of, CMN has responsibility for ensuring data is collected, stored and handled appropriately, the Company's ICT Policy also takes into account Data Protection and GDPR.

14.2 CMN's Data Protection Officers /data controllers are responsible for reviewing this policy and updating Directors on the CMN's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

14.3 Personal data, as covered by this policy, should only be accessed by personnel who have been given specific permission to access data as part of their role/ permission, in accordance with their working routines. Data should only be used for the specified lawful purpose for which it was obtained.

14.4 You should not share any personal data informally.

14.5 You should keep all personal data secure and not share it with unauthorised people.

14.6 CMN regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

14.7 Personal data should never be transferred outside the UK except in compliance with the law and authorisation of the CMN Data Protection Officer.

14.8 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

14.9 You should not take personal data away from CMN's premises without authorisation from your line manager or the CMN's Data Protection Officer.

14.10 Personal data should be shredded and disposed of securely when you have finished with it.

14.11 You should ask for help from the CMN's Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security, we can improve upon.

14.12 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

14.13 It is a criminal offence to conceal or destroy personal data, which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

15 How to deal with data breaches

15.1 CMN have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals', then CMN must also notify the Information Commissioner's Office within 72 hours.

15.2 If you are aware of a data breach, you must contact your line manager or the PA to CEO and Claims and Administration Manager immediately and keep any evidence you have in relation to the breach.

16 Subject access requests

16.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the Data Protection Officer who will coordinate a response.

16.2 If you would like to make a SAR in relation to your own personal data, you should make this in writing to your line manager. CMN must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

16.3 There is no fee for making a SAR. However, if your request is manifestly unfounded (if the individual has no clear intention to access the information or is malicious in intent and is using the request to harass an organisation with no real purposes other than to cause disruption) or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

17 Your data subject rights

17.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

17.2 You have the right to access your own personal data by way of a subject access request (see above). There are a small number of exemptions which include:

- Data about you that is used for management forecasting and planning;
- Data about you that may be used in negotiations with you;
- Data that could disclose a trade secret;
- Data about you that is subject to legal professional privilege;
- Data that discloses the identity of third parties unless their prior **informed consent** is received.

17.3 You can correct any inaccuracies in your personal data. To do you should contact your line manager, or the PA to CEO and Claims and Administration Manager.

17.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was

collected. To do so you should contact your line manager, or the PA to CEO and Claims and Administration Manager.

17.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact your line manager, or the PA to CEO and Claims and Administration Manager.

17.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

17.7 You have the right to object if we process your personal data for the purposes of direct marketing.

17.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

17.9 With some exceptions, you have the right not to be subjected to automated decision-making.

17.10 You will be notified of a data security breach concerning your personal data.

17.11 In most situations, we will not rely on your consent as a lawful ground to process your data. If CMN does however request your **informed consent** to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your **informed consent** later. To withdraw your consent, you should contact your line manager, or the PA to CEO Claims and Administration Manager.

17.12 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

18Privacy audits

18.1 Cornwall Marine Network Ltd. will conduct a Data Protection audit at least once a year. Under the Data Protection Act, personal data shall be processed according to six principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

18.2 These are underpinned by the principle of accountability. The data controller will keep certain records to demonstrate CMN's compliance.

18.3 An audit should consider the extent to which data protection accountability, responsibility, policies and procedures, performance measurement controls and reporting mechanisms are in place and operating throughout CMN.

18.4 CMN takes a risk-based approach to implementing "appropriate technical and organisational measures", which includes conducting DPIAs (data protection impact assessments) in certain circumstances. DPIAs are a type of risk assessment that identifies the risks to and likely effects of processing on the security of personal data. These audits should examine:

- Whether privacy risk is included in your corporate risk register;
- What corporate arrangements for privacy risk management are in place;
- To what extent the corporate risk regime incorporates information-specific risks; and
- Which risks to the rights and freedoms of natural persons are addressed.

19 How to perform a data audit

19.1 When conducting an audit, CMN should take into account several key questions about the data we hold and document our findings. Things CMN should consider include:

20 What types of personal data do you hold

20.1 List the categories of data subjects and any personal data, which CMN collects. For example, current employee data,

- past employee data,
- customer data,
- marketing database,
- CCTV footage, etc.

20.2 This data is segmented by type, e.g. people's names, addresses, purchasing history, online browsing history, images etc. Determine if CMN hold just personal data, or does some of it fall under the category of sensitive personal information? Does CMN collect and process children's data?

21 Why do you hold this data

21.1 List the purposes for which CMN collects and retains this data. For example, marketing, service improvements, product development, human resources, systems maintenance, etc.

- Consider what CMN does with the data?
- Does CMN use it at all? Do CMN need it?
- Can CMN show what you use it for?

21.2 Establish the exact purpose and the lawful basis for processing of personal data (e.g. consent, contract, legal obligation, etc.).

22 How did you collect this data

22.1 List the sources of personal data. For example,

- Did CMN collect it directly from individuals or third parties?
- Can CMN show the different methods used to collect data?
- Does CMN have a documented consent / opt-in?
- Has CMN communicated your privacy policy to data subjects?

23 How do you store it

- Can CMN show how and when they collected the data?
- Can CMN document where they store it?
- How do CMN protect and access it?
- How secure is the data, both in terms of encryption and accessibility?

24 What do you do with this data

- How does CMN process it?
- Does CMN share it with anyone?
- Why does CMN share it?
- Does CMN transfer personal data outside of the UK?

25 Who owns and controls the data

- Do CMN have a controller or processor of the data?
- Who has access to it (internally and externally)?
- What safeguards does CMN have in place with your processors?

26 How long do you keep the data for

26.1 Check CMN's retention and deletion periods. What justification do CMN have for the length of time they retain it? What is CMN's process for deleting data?

27 What CMN need to do to make your data processing GDPR compliant

27.1 List actions that CMN should do to ensure they processing is compliant with the legislation. For example, do we need to delete data that has exceeded the retention period or data CMN have collected un-lawfully.

27.2 It may help to put all this information in a spreadsheet or a word document, including specific headings for each of these considerations.

28 Data audit templates

28.1 The Information Commissioner's Office (ICO) has developed basic templates which CMN has adopted, these document CMN's processing activities.

29 Training

29.1 All new employees, workers, volunteers, apprentices, contractors and consultants, will as part of their induction process, training will be given on this policy. Further to this, refresher training will be given annually or following any update to the policy.

Approved by: Lucy Harris, Operations Director

Version	Date	Responsible	Changes
1.1	2019	Tim Salmon	Initial creation
1.2	Sept 2020	Tim Salmon	Annual refresh
1.3	October 2021	Chris Freer	Review, updates, remove EU
1.4	October 2021	Lucy Harris	Minor edits, version control and approval
1.5	December 2022	Chris Freer	Annual review and minor amendments
1.6	February 2023	Chris Freer	Further review and ensure coverage of additional points
1.7	April 23	Lucy Harris	Interim DPO appointment
1.8	May 23	Lucy Harris	Enhanced reference to UK GDPR
1.9	June 23	Lucy Harris	Amendment of DPO and formatting