**FQM LIMITED**

**XXX-OP-015**

**GDPR**

1. **PRIVACY STATEMENT – DALES MARINE SERVICES**
	1. **Introduction**

[COMPANY NAME] take seriously our obligation to protect sensitive information and data relating to our clients, suppliers and partner businesses. This document details our policy for handling data as defined by the General Data Protection Regulation (“GDPR”) and the purposes for which we will share such information.

Our overriding policy is one of fairness and accountability. If you have any questions regarding our data protection and privacy policy please ask a member of staff/HR Department.

* 1. **Collecting Personal Information**

We may collect, store and use the following kinds of personal information:

**Customers:**

* information that you provide to us when registering with our website (including your email address);
* information that you provide when completing an online enquiry via social media (Facebook, Twitter, Google etc.) including your name, gender, date of birth and any educational details and employment details you provide;
* information that you provide to us when signing up to any distribution lists to receive correspondence from us;
* information relating to any purchases you make of our goods or services, including any other transaction details made via any of our websites, in person or over the phone (including your address, telephone number and payment details);
* information you provide when visiting our showroom or using our demonstrator vehicles.
* information you provide when using a loan vehicle;
* information passed to us by our partner businesses, manufacturers and suppliers where you have given them permission to do so; and
* digital images captured by CCTV equipment.

**Staff:**

* Personal information of employees, contractors and their next of kin in relation to HR matters.

**Consent:**

We will always obtain your consent to use your personal information. This will be an explicit consent from you. In certain areas of our business withholding your consent will prevent us from completing a transaction. This would include the sale of vehicles, applications for finance, completion of warranty claims, applications for credit accounts, provision of service plans and the purchase of insurance based products.

* 1. **Using Personal Information**

Personal data we receive will be used for the purposes for which it was provided, including:

* to meet the terms of your order for goods or services;
* to enable your use of the services available on our website;
* to send you goods purchased through our website or by phone;
* to supply to you services purchased through our website, in person or by phone;
* to send statements, invoices and payment reminders to you, and collect payments from you;
* to send you our newsletter, promotional mailings and service reminders (you can inform us at any time if you no longer require the newsletter) in any format including electronic; and,
* to provide third parties with statistical information about our users (but those third parties will not be able to identify any individual user from that information).
	1. **Disclosing Personal Information**

We may disclose your personal information:

* to any of our staff, agents, suppliers or subcontractors where it would be reasonable to do so. (If consent is necessary to facilitate this sharing we will ensure it is obtained prior to processing);
* to any member of our group of companies where it would be reasonable to do so. (If consent is necessary to facilitate this sharing we will ensure it is obtained prior to processing);
* to the vehicle manufacturer in relation to ownership, warranty and marketing purposes; and,
* to finance companies in the application for finance, leasing or related products. This will only be in response to a direct request from you.

We may be legally obliged to disclose your personal information:

* to the extent that we are required to do so by law;
* in connection with any ongoing or prospective legal proceedings;
* in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk); and
* to any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.

Except as provided in this policy, we will not provide your personal information to third parties.

* 1. **Security of Personal Information**
* We will take all reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.
* We will store all the personal data you provide on our secure servers.
* All personal information shared electronically will be encrypted or sent via secure connections.
* We will protect hard copies of your personal data in a secure fashion.
	1. **Your Rights**
* You may instruct us to provide you with any personal information we hold about you, via a Subject Access Request
* Upon receipt of such a request we will, after confirming identity, provide all relevant data we hold to you in the most practical format unless otherwise stipulated and reasonably possible.
* We may withhold personal information that you request to the extent permitted by law.
* If you instruct us to no longer process your personal data we will do so as quickly as possible.
* If you instruct us to destroy any/all of your personal data we may hold we will do so as quickly as possible. This will exclude our legal requirement to hold information for audit, VAT and taxation purposes.
* If you instruct us to cease all processing for marketing purposes we will do so as quickly as possible.

Where we see a demonstrable and legitimate need to contact you, contrary to these instructions, (for example in relation to vehicle safety or a manufacturers recall campaign) we will do so for information purposes only.

* 1. **Cookies**

Our website, and those of our partner businesses, may use cookies to facilitate faster loading times and to record personal information. Access to our website requires the use of cookies. If you do not wish to have information recorded please follow the guidance available in your web browser to delete them.

* 1. **ICO Registration**

We are registered as a data controller with the Information Commissioner's Office and our registration number is: xxxxxxxx

* 1. **Data Protection Officer**

Our Data Protection Officer is xxxxxxx. He may delegate operational duties to suitably competent persons in the routine operation of our business. Any Data Protection issues can be directed to xxxxxxxxx.

1. **CLEAR DESK AND CLEAR SCREEN POLICY**
	1. **Policy Statement**

A clear desk and clear screen policy reduces the risks of unauthorised access, loss of and damage to information during and outside normal working hours. The Data Protection Act 1998 and GDPR require the protection of unauthorised access to sensitive data.

Additionally, much of [COMPANY NAME] data must be protected according to legal and contractual requirements.

* 1. **Scope and Application of the Policy.**

This policy applies to all [COMPANY NAME] employees and any other person utilising any form of information technology or having responsibility for institutional information stored in an alternative format, such as paper.

This policy covers any papers, removable storage media and any computing devices that contain or display information in the care of [COMPANY NAME] regardless of location.

* 1. **Definitions.**
* “Screen” shall mean the display portion of any computing device.
* “Public area” shall mean a location outside of a lockable office where the general public has free and easy access to the area.
* “Secured” shall, at the very least, mean the locking of or otherwise preventing access to information, records, and/or physical space.
	1. **Clear Desk and Clear Screen Policy.**

The following security measures must be followed:

* Whenever unattended or not in use, all computing devices must be left logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism (this includes laptops, tablets, smartphones and desktops).
* When viewing sensitive information on a screen, users should be aware of their surroundings and should ensure that third parties are not permitted to view the sensitive information.
* Sensitive or critical business information, e.g. on paper or on electronic storage media, must be secured when not required, especially when the office is vacated at the end of the work day.
* Paper containing sensitive or classified information must be removed from printers and faxes immediately. Faxes and printers used to print sensitive information should not be in public areas. Any time a document containing sensitive information is being printed the user must make sure they know the proper printer is chosen and also go directly to the printer to retrieve the document.
* Sensitive information on paper or electronic storage media that is to be shredded must not be left in unattended boxes or bins to be handled at a later time, and must be secured until the time that they can be shredded.
* In the event that any personal data is lost, misplaced or stolen you shall inform your line manager and the data controller immediately.
	1. **Review**

This procedure will be reviewed on a regular basis, at a minimum on a yearly basis. Additional review may be required due to changes in legislation, operations, technology, personnel etc.

1. **PORTABLE ELECTRONIC DEVICE SECURITY**
	1. **Policy Statement**

This document describes the policy for ensuring the secure storage and management of confidential data and personal information belonging to Dales marine Services Ltd held on or accessed via portable devices and storage media. The GDPR and Data Protection Act (“DPA”) require the protection of unauthorised access to sensitive data.

Additionally, much of [COMPANY NAME] data must be protected according to legal and contractual requirements.

* 1. **Scope and Application of the Policy**

This policy applies to all [COMPANY NAME] employees and any other person utilising any form of information technology.

This policy includes all forms of portable device designed, adapted or capable of storing, transferring or accessing digitally stored data.

* 1. **Definitions.**
* Portable Device: Hand-held and other hand-portable computing equipment which is used for accessing, storing or processing Dales Marine Services Ltd data, including (but not limited to) laptop PCs, tablets, mobile telephones and PDAs.
* Portable Media: Readily-transportable items used to store data in electronic form (whether temporarily or long-term), including data sticks (“flash drives”), floppy disks, compact discs (CDs and DVDs), plug-in external drives and media players (mp3 players).
* Confidential Data: Information about or connected with the Dales Marine Services Ltd business (including Personal Data and Sensitive Personal Data, as defined below) which the user has an obligation to treat as confidential and protect from unauthorised use, access or release.
* Personal Data: Means any information about any living, identifiable individuals.
* Sensitive Personal Data: Is a sub-set of Personal Data, and means personal information about an individual’s racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life; commission or alleged commission of any offence; any proceedings for any offence actually or allegedly committed by that individual, the disposal of such proceedings or the sentence of any court in such proceedings.
* User: A member of Dales Marine Services Ltd staff or other person making authorised use of a portable device or portable media to store, access or manipulate Confidential Data.
	1. **Portable Electronic Device Security Policy**
1. **General duty to protect data**
2. All [COMPANY NAME] employees and those who are formally engaged to work or act on behalf of the company have a contractual obligation to take adequate steps to prevent unauthorised use or disclosure of Confidential Data and must take reasonable care to protect the portable device or media from loss or theft.
3. In addition, the protection of Personal Data is a legal obligation imposed by the GDPR. A breach of that obligation can bring significant financial penalties and other sanctions for those responsible. The GDPR requires adequate steps to be taken to protect Personal Data, with even greater care expected to protect Sensitive Personal Data in view of its private nature.
4. Sensitive Personal Data must not be stored on a portable device or media except as provided for in section B III.
5. A breach of this Policy may result in serious disciplinary action using the Dales Marine Services Ltd Disciplinary procedure, irrespective of any penalties or sanctions which may be imposed by the Information Commissioner in respect to any failure to protect personal or sensitive personal data.
6. **Minimising the transfer of Confidential Data to portable devices and media.**
7. As a general principle, Confidential Data should be held securely on the Dales Marine Services Ltd core systems, should be accessed and managed using only those systems, and should not be downloaded for storage or remote manipulation on portable devices or media
8. Wherever available, secure online file transmission procedures must be used in preference to portable media to send Personal Data directly to authorise external recipients.
9. In the event that it becomes essential to place confidential data on a portable device or media or where use of portable media is the only viable option for transferring data transfer, the user must ensure that the portable device or media must meet the minimum protection criteria specified in Section C below.
10. Data copied to portable devices or media must be deleted at the earliest opportunity. Where the data was commercially sensitive or contained Personal Data deletion must be by means of an overwrite tool to prevent future recovery.
11. All staff opting to use personal devices to access email accounts belonging to Dales Group companies, regardless of the trading name, agree to permit access to their device upon the cessation of their employment for any reason. This will be to ensure all locally held email content sent or received over company addresses is deleted.
12. Personal Data must never be stored in unprotected form on portable devices or media.
13. **Minimum protection criteria.**

|  |  |
| --- | --- |
| Device or Media type | Security requirement |
| Laptop PC, Tablet or equivalent | Device must be protected by a password containing a minimum of 8 characters and this must include a mixture of capitalisation, symbols and numbers.Files containing sensitive or personal data must be individually protected by passwords. |
| Mobile Phone | Power on password/pin and auto lock activated. Biometric security is acceptable. |
| Memory stick, SD card or equivalent | All files must be password protected. If used for sensitive or personal data then device based encryption must be used. |
| Other devices which allow storage of files i.e. iPad, iPod. | These devices should not be used to store sensitive or personal data. |

* 1. **Action To Be Taken In The Event Of Actual Or Suspected Loss Of Confidential Data**
* The user must immediately notify their line manager and the data controller of the occurrence of any of the following and comply with reasonable instructions or directions from them to minimise any attendant risk:
* Theft or loss of a portable device on which Confidential Data was stored or could be accessed;
* Theft or loss of portable media containing Confidential Data, including media sent to an external recipient which has failed to reach its destination;
* Actual or suspected use of the user’s portable device to gain unauthorised access to Confidential Data;
* Any other incident involving a portable device or media under the user’s control which represents an actual or potential compromise to the security of Confidential Data. Other supporting documents and material.
	1. **Review**

This procedure will be reviewed on a regular basis, at a minimum on a yearly basis. Additional review may be required due to changes in legislation, operations, technology, personnel etc.

1. **SUBJECT ACCESS REQUEST POLICY (SAR)**
	1. **Policy Statement**

This document represents our policy for responding to Subject Access Requests (SARs) under the General Data Protection Regulations (GDPR).

* 1. **Scope and Application of the Policy.**

This policy applies to all [COMPANY NAME] employees.

* 1. **What is a SAR?**

A SAR is the most commonly exercised right currently available to individuals under the present Data Protection Act 1998 and will be expanded and strengthened under the soon to be implemented GDPR. It is the principal avenue of access for individuals who wish to obtain and view the amount or level of personal data an organisation may hold on them.

It represents a formal request from an individual obligating you to assess all of the personal data you hold and collate that which is relevant to the requester. This is a fundamental right of the Data Protection Act 1998 (DPA) and one which you are legally bound to respond to.

The GDPR will give individuals a right to obtain:

* Confirmation that their personal data is being accessed
* Access to that personal data being held
* Any other information which would be of assistance (list those you have shared data with for example)
	1. **How Will SARS be Submitted?**

A SAR is a written request for personal information (known as personal data) held about an individual. Generally, individuals have the right to see what personal information is held about them and they are entitled to be given a description of the information, what it is/was used for and who it may have been shared with. However, this right is subject to certain exemptions that are set out in the GDPR.

* 1. **What do we do When we Receive a SAR?**

The first step is to ensure the identity of the requester, which can be confirmed by asking for two forms of identity, one of which must be photographic (driver’s licence, passport, bus pass etc.) and one which must confirm the requester’s home address. Once received the process of gathering any data held can begin. While this is the generally accepted method of validating identity, all the GDPR states that you need to be satisfied that the applicant is who they claim to be. As such if a SAR is submitted to you via email, and you hold the individual’s telephone number, a call asking for confirmation of the request would be deemed sufficient.

Once we have enough information from a requester to identify any relevant records we will collate all the detail we hold. If we feel we need more information from the requester we must contact them promptly asking for this.

Once we have completed the data gathering a permanent copy of the relevant data will be forwarded to the requester, usually via the method by which they submitted their original request.

* 1. **What is Personal Data?**

The Information Commissioner’s Office (ICO) defines data as:

Personal data means data which relate to a living individual who can be identified:

* From those data, or
* From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data consisting of information as to:

* The racial or ethnic origin of the data subject,
* His/her political opinions,
* His/her religious beliefs or other beliefs of a similar nature,
* Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
* His/her physical or mental health or condition,
* His/her sexual life,
* The commission or alleged commission by him/her of any offence, or
* Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Taken from the actual legislative document representing the GDPR personal data is defined as:

* ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
* Any information which falls under any of the above headings will be deemed relevant when handling a SAR.
	1. **Can we Charge a Fee?**

A ‘reasonable fee’ can be charged in instances where a request is deemed manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information and it is suggested that any fee charged should be in line with the costs incurred whilst supplying the information requested. If a fee is to be charged we must inform the requester as early as possible following consultation with a manager.

Where requests are manifestly unfounded, excessive or repetitive we are entitled to charge a reasonable fee in respect of providing the information; or we can refuse to respond. Where a request is refused an explanation of why must be provided to the requester alongside information detailing their right to complain to the supervisory authority (the ICO).

* 1. **What is the Timeframe for Responding to SARS?**

The response deadline has been reduced under the GDPR which stipulates that information must be provided without delay and at the latest within one month of receiving a request.

However, there is scope to extend the response deadline by an additional two months when handling particularly complex or numerous requests. In such instances contact must be made with the requester explaining why the extension is necessary.

* 1. **What About Personal Data Held by Credit Reference Agencies?**

If we receive a request for information contained within a credit reference file we must inform the requester that we are unable to comply with their request and provide them with contact details for the finance company(s) who make the lending decision.

* 1. **Complaints**

It is an expectation that as part of responding to an SAR you inform the individual of how they can complain if they are unhappy. Provision of the contact details for the ICO should be included as follows:

If you are dissatisfied with our response you can complain to the Information Commissioner's Office via the following:

xxxxxx

* 1. **Review**

This procedure will be reviewed on a regular basis, at a minimum on a yearly basis. Additional review may be required due to changes in legislation, operations, technology, personnel etc.

1. **Data Path Accompanying Notes**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Company Name** |  | **Dept** |  | **Name** |  | **Date** |  |
| Original data source | Physical Data capture? | Electronic data capture? | External system transfer? | External system transfer? | External system transfer? | External system transfer? | Archiving paper records? |
|  | Consent requested? | Consent suitable for data type? | Consent suitable for data type and transfer? | Consent suitable for data type and transfer? | Consent suitable for data type and transfer? | Consent suitable for data type and transfer? | Is file physically secure? |
|  | Where and how long is this stored? | How does system provider store data? | How does system provider store data? | How does system provider store data? | How does system provider store data? | How does system provider store data? | How long is file stored? |

As part of the forthcoming GDPR changes all group companies will be required to complete a data audit. The above form, attached in Excel, will be the template used.

By department each manager must consider how there area of the business obtains and manages personal data and must maintain an auditable record of this.

The example document was completed for xxxxx sales department as a reference guide.

In the 1st line of boxes the relevant manager should complete the company and department details and enter their name and the date of completion. 1 sheet is required per source of data.

The original data source is the point at which we obtain personal information, this could be in person, by phone or in digital format via email, web enquiries or social media channels.

Physical capture refers to non-electronic records such as diaries, order forms and job cards. Electronic capture is any computer based system that may include mobile devices whether or not they belong to the business e.g. personal mobile containing a business contact or data.

Electronic transfer is the sharing of personal data out with the business, for example sending data to a 3rd party supplier, warranty agent or accounts firm.

Archiving paper records, yes or no.

The second row of questions covers obtaining consent to hold, process and share the data. Consider your privacy policy. If you plan to hold, transfer or use the data to market the person, you must obtain explicit consent.

The end column asks you to consider physical security of archived documents.

The 3rd row considers the validity of consent over a period of time and the method of data storage. IF you send the data to a 3rd party you will need consent to do so AND a statement from the 3rd party confirming what they intend to do with the data.

The end column refers to archived physical records.

Once completed these documents should be compiled into a single spreadsheet with each tab titled by the data source and department e.g. “sales department walk in” and the completed document returned to Chris.

These data audits are required to be updated when changes occur that affect the handling of personal data.